ExtremeXOS Release Notes

Software Version ExtremeXOS 12.6.2-patch1-9

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: March 2012
Part Number: 120654-00 Rev 14

AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2012 Extreme Networks, Inc. All Rights Reserved.

Contents

Chapter 1: Overview 5

Feature Corrections in ExtremeXOS 12.6.2 5
New Features and Functionality in ExtremeXOS 12.6.1 6
New Hardware Supported in ExtremeXOS 12.6.1 9
Hardware No Longer Supported 9
Supported Hardware 10
BlackDiamond 8800 Series of Switches Component Support 10
BlackDiamond 10808 Switch Component Support 11
BlackDiamond 12800 Series Switches Component Support 12
BlackDiamond 20800 Series Switch Component Support 13
Summit X150 and X350 Component Support 14
Summit X250e Component Support 15
Summit X450a and X450e Component Support 15
Summit X460 Component Support 16
Summit X480 Component Support 16
Summit X650 Component Support 17
SFP (Mini-GBIC) Support 17
XENPAK Module Support 23
XFP Module Support 25
Upgrading to ExtremeXOS 27
Downloading Supported MIBs 27
ExtremeXOS Command Line Support 27
Tested Third-Party Products 27
Tested RADIUS Servers 27
Tested Third-Party Clients 28
PoE Capable VoIP Phones 28
Extreme Switch Security Assessment 29
DoS Attack Assessment 29
ICMP Attack Assessment 29
Port Scan Assessment 29

Chapter 2: Limits 31

Supported Limits 31

Chapter 3: Open Issues, Known Behaviors, and Resolved Issues 67

Open Issues 67
Known Behaviors 81
Resolved Issues in ExtremeXOS 12.6.2-patch1-9 84
Resolved Issues in ExtremeXOS 12.6.2-patch1-8 84
Resolved Issues in ExtremeXOS 12.6.2-patch1-6 85
Resolved Issues in ExtremeXOS 12.6.2-patch1-5 86
Resolved Issues in ExtremeXOS 12.6.2-patch1-3 88
Resolved Issues in ExtremeXOS 12.6.2-patch1-2 90
Resolved Issues in ExtremeXOS 12.6.2 92
Resolved Issues in ExtremeXOS 12.6.1 95

1 CHAPTER Overview

These Release Notes document ExtremeXOS® 12.6.2-patch1-8 which resolves software deficiencies.

This chapter contains the following sections:

- Feature Corrections in ExtremeXOS 12.6.2 on page 5
- New Features and Functionality in ExtremeXOS 12.6.1 on page 6
- New Hardware Supported in ExtremeXOS 12.6.1 on page 9
- Hardware No Longer Supported on page 9
- Supported Hardware on page 10
- Upgrading to ExtremeXOS on page 27
- Downloading Supported MIBs on page 27
- Tested Third-Party Products on page 27
- Extreme Switch Security Assessment on page 29

Feature Corrections in ExtremeXOS 12.6.2

This section lists the feature corrections supported in ExtremeXOS 12.6.2 software:

- **ESRP over IPv6 Support**—The ExtremeXOS software now supports Extreme Standby Router Protocol™ (ESRP) operation over IPv6 networks. Configuration and operation is similar to that documented in the *ExtremeXOS Concepts Guide* and *ExtremeXOS Command Reference Guide* with the following exceptions:
  - The ESRP VLAN configuration on each ESRP master and slave must have both an IPv6 and an IPv4 address.
  - ESRP route tracking is not supported on IPv6 networks.
  - ESRP Ping tracking is not supported on IPv6 networks.

New Features and Functionality in ExtremeXOS 12.6.1

This section lists the new features and functionality in ExtremeXOS 12.6.1:

- **ARP Filtering—**This feature adds two new access list match criteria:
  - `arp-sender-address <prefix>`
  - `arp-target-address <prefix>`

  Available on BlackDiamond 8800 series switches and Summit family switches only.
- **Customer Edge Port —**This feature, also known as Selective Q-in-Q, adds the ability for a VMAN customer-facing port to associate only frames containing configured Customer VLAN IDs (CVIDs) with a VMAN. In addition, it allows frames from the same customer-facing port but containing different CVIDs to be associated with different VMANs. Previously, frames from a given VMAN customer-facing port could be associated to only one VMAN.
  - IEEE 802.1ad Customer Edge Port (also known as 802.1ad C-tagged service interface and MEF UNI Type 1.2) data plane on Summit and BlackDiamond 8000 series switches.
  - 1-to-1 and N-to-1 CVID-to-VMAN mappings.
  - Multiple CVID-to-VMAN mappings to different VMANs per customer facing port.
  - CVID translation (for example, translation between CVID X on the customer-facing port and CVID Y in the VMAN encapsulation).
  - Configuration via CLI, not ACL policy file.
  - Limited coexistence of Customer Edge Port interfaces with tagged VLAN interfaces, an untagged VMAN interface, and tagged VMAN interfaces on the same port.
- **Data Center Solutions Updates—**This feature now includes the following changes:
  - Repository server configuration updates that affect configuration and support password authentication.
  - New support for DCBX—The Data Center Bridging eXchange (DCBX) protocol is used by Data Center Bridging (DCB) devices to exchange DCB configuration information with directly connected peers. In an ExtremeXOS enabled switch, the switch uses DCBX to advertise its DCB configuration to end stations. The end stations can then configure themselves to use the switch DCB services. If the peers do not support a common configuration for one or more features, the switch generates messages to alert network management.

    The DCBX protocol advertises the following types of information:
    - DCBX version information, so that the peers can negotiate a common version to use.
    - Enhanced Transmission Selection (ETS) information for QoS parameters such as bandwidth allocation per traffic class (802.1p COS), priority for each traffic class, and the algorithm used for servicing traffic classes.
    - Priority-based Flow Control (PFC) information for managing flow control between peers.
    - Application priority information for prioritizing traffic for special applications that do not map directly to an established traffic class.
- **Display Time Stamp for Last Port Up/Down Transition—**The `show port info detail` command now displays the date and time of the last physical port link state transition (Up or Down).
- **Display VLAN Information by Tag—**This feature adds the keyword `tag` as a qualifier to the following CLI VLAN, vMAN, and port-related `show` commands. The `tag` option allows you to specify the interfaces to be displayed by entering the 802.1Q tag value. The display output format remains unchanged.
  - `show ports`
  - `show ports anomaly`

- show ports collisions
- show ports configuration
- show ports information
- show ports ip-fix
- show ports network-clock sync-e
- show ports packet
- show ports transceiver information
- show ports transceiver information detail
- show ports utilization
- show ports wan-phy configuration
- show ports wan-phy errors
- show ports wan-phy events
- show ports wan-phy overhead
- show vlan
- show vman
- show bvlan
- show svlan
- show cvlan
- show learning-domain

- **Duplicate IP Address Detection (DAD) and Prevention**—This feature detects and prevents duplicate IP addresses during VLAN initialization. If the switch detects another device that is using the IP address assigned to the VLAN, the switch disables the IP address for the VLAN and generates an EMS log message. This action can occur only during initialization of the VLAN. If the switch later detects a duplicate IP address, the duplicate IP address on the switch is not disabled.

NOTE

IP DAD CLI commands are only supported on the Summit family and BlackDiamond 8800 series switches.

For IPv4 networks, this feature is disabled by default to match the behavior of earlier versions of the ExtremeXOS software. You can use the `configure ip dad [off | on | {on} attempts <max_solicitations>] {{vr} <vr_name> | vr all}` command to configure this feature, and you can use the `run ip dad [{vlan} <vlan_name> | {{vr} <vr_name>} <ipaddress>]` command to initiate a DAD check after initialization. To view the status of the DAD feature, use the `show ip dad {[{{vr} <vr_name> {<ip_address>} | vr all | {vlan} <vlan_name>}` command. To clear the DAD feature counters, use the `clear ip dad {{vr} <vr_name> {<ipaddress>} | vr all | {vlan} <vlan_name>} {counters}` command.

For IPv6 networks, this feature is enabled by default to match the behavior of earlier versions of the ExtremeXOS software, which supported the DAD feature, but did not provide commands to manage this feature. You can use the `configure ipv6 dad [off | on | {on} attempts <max_solicitations>] {{vr} <vr_name> | vr all}` command to configure this feature, and you can use the `run ipv6 dad [{vlan} <vlan_name> | {{vr} <vr_name>} <ipaddress>]` command to initiate a DAD check after initialization. To view the status of the DAD feature, use the `show ipv6 dad {[{{vr} <vr_name> {<ip_address>} | vr all | {vlan} <vlan_name>} {tentative | valid | duplicate} | {{vr} <vr_name>} <ipaddress>]}` command. To clear the DAD feature counters, use the `clear ipv6 dad {{vr} <vr_name> {<ipaddress>} | vr all | {vlan} <vlan_name>} {counters}` command.

- **Filtering the Output of "show" Commands**—This feature is a restricted version of a UNIX/Linux feature that uses a "pipe" character to direct the output of one command to be used as input for the next command. It provides support for "piping" `show` command output to the display filter using the vertical bar (`|`) operator. In the following command, it is the first vertical bar. The display filter displays the output based on the specified filter keyword option and the text pattern entered. By selecting different filter options you can include or exclude all output that matches the pattern. You can also exclude all output until a line matches the pattern and then include all output beginning with that line.

  In ExtremeXOS software, the resulting command is as follows:

  ```
  show <specific show command syntax> | {include | exclude | begin} <regexp>
  ```

  The following describes the command syntax:

`show <specific show command syntax>`	State the command. For example: `show ports`.(This is followed by the vertical bar (|) when used as the pipe character.)
`include`	Display the lines that match the regular expression.
`exclude`	Do not display the lines that match the regular expression.
`begin`	Display all the lines starting with the first line that matches the regular expression.
`regexp`	The regular expression to match. • Regular expressions are case sensitive. • It is common to specify your regular expression in quotes

  For example, using the following command:

  ```
  show ports 2:1-2 information detail | include "(Port|Flow Control)"
  ```

  The output would resemble the following:

  ```
  Port: 2:1
       Flow Control:   Rx-Pause: Enabled       Tx-Pause: Disabled
       Priority Flow Control: Disabled
  Port: 2:2
       Flow Control:   Rx-Pause: Enabled       Tx-Pause: Disabled
       Priority Flow Control: Disabled
  ```

- **Identity Management Updates**—This feature now includes the following changes:
  - Added support to detect FDB entries as identities (unknown identities)
  - Changed default behavior to manage entries based on the MAC address, instead of by IP address
  - Added support to age-out Kerberos users during periods of inactivity
  - Added support for Kerberos to force age-out
- **LLDP Neighbor Refresh Command**—A new CLI command, `clear lldp neighbor [all | port <port>]`, allows a user to flush all neighbor information, or flush neighbor information on a port basis. Prior to this command, LLDP neighbor entries could only be cleared by aging out.
- **STP Description**—This feature provides support for adding an STP domain description. An optional description keyword is now included in the `create stpd` and `configure stpd` commands. The STP domain description is shown in the output of the `show` command.
- **Supported Hardware**—The supported hardware section previously included in the ExtremeXOS release notes is now a standalone document The the *.xos file names have also been removed.

https://www.extremenetworks.com/libraries/services/HW_SW_Compatibility_Matrix.pdf

- **Tunable DWDM, 50-GHz**—ExtremeXOS software now supports tunable dense wavelength division multiplexing (TDWDM) XFP modules with 50-GHz channel spacing. The feature is supported on BlackDiamond 8800 switches with 10G8Xc, 10G4Xc, 10G4Xa or 8900-10G8Xxl modules and S-10G1Xc option cards, BlackDiamond 20800 series switches with XM-8XB or HM-2X24GA modules, and Summit X480 switches with VIM2-10G4X modules.
- **VLAN Description**—A VLAN description is a string of up to 64 characters that you can configure to describe the VLAN. The keyword `description` is now included in the `create` and `configure` commands. For example, `create vlan <vlan_name> {description <vlan-description>} {vr <name>}` and `configure vlan <vlan_name> {description <vlan_description>}`. The description length is 64 characters; the VLAN description is displayed in the output of the `show` command.
- **XNV™**—The Extreme Network Virtualization (XNV) feature, which is also known as Virtual Machine (VM) tracking, enables the ExtremeXOS software to support VM port movement, port configuration, and inventory on network switches. VM movement and operation on one or more VM servers is managed by a VM Manager (VMM) application. The XNV feature enables a network switch to respond to VM movement and report VM activity to network management software.

New Hardware Supported in ExtremeXOS 12.6.1

The following hardware is supported in ExtremeXOS 12.6.1:

- BlackDiamond 8800 series switch
  - 8900-40G6X-xm (6 x 40G I/O module)
- Summit X650 series switch
  - VIM3-40G4X (4 x 40G option card)
- Summit X670 series switch
  - Summit X670V-48x (48 x 10-Gb Summit stackable capable of 4 x 40-Gb)
  - Summit X670-48x (48 x 10-Gb Summit stackable)
  - VIM4-40G4x (4 x 40-Gb option card for Summit X670V-48x)
  - VIM3-40G4x (4 x 40-Gb option card for Summit X650-24t and Summit X650-24x)

Hardware No Longer Supported

The following hardware is no longer supported in ExtremeXOS 12.6.1:

- MSM-G8X
- MSM-48

Supported Hardware

Refer to the Extreme Networks hardware installation guides for more information about supported hardware. The following tables list the software filenames for the hardware that requires software.

BlackDiamond 8800 Series of Switches Component Support

BlackDiamond 8800 and BlackDiamond 8806 components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the chassis to support each component, include:

Table 1: BlackDiamond 8800 Series of Switches Component Support

BlackDiamond 8810 and BlackDiamond 8806 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-G8X	bd8800-12.5.4.5-patch1-6.xos	11.1.1.9	1.0.1.7
MSM-48	bd8800-12.5.4.5-patch1-6.xos	11.6.1.9	1.0.1.11
MSM-48c	bd8800-12.5.4.5-patch1-6.xos	12.1.1.4	1.0.3.7
8500-MSM24	bd8800-12.5.4.5-patch1-6.xos	12.3.1	1.0.4.2
8500-G48T-e	N/A	12.3.1	1.0.4.0
8500-G24X-e	N/A	12.3.1	1.0.4.0
8900-MSM128	bd8800-12.5.4.5-patch1-6.xos	12.3.1	1.0.4.2
8900-10G24X-c	N/A	12.3.1	1.0.1.0
8900-G96T-c	N/A	12.3.2	1.0.1.0
8900-G48X-xl	N/A	12.4.1	1.0.1.2
8900-G48T-xl	N/A	12.4.1	1.0.1.2
8900-10G8X-xl	N/A	12.4.1	1.0.1.2
G48Te	N/A	11.5.1.4	1.0.1.10
G48Pe	N/A	11.5.1.4	1.0.1.10
G48Ta	N/A	11.5.1.4	1.0.1.10
G48Xa	N/A	11.5.1.4	1.0.1.10
G48Tc	N/A	12.1.1.4	1.0.3.7
G48Te2	N/A	12.1.1.4	1.0.3.7
G48Xc	N/A	12.1.1.4	1.0.3.7
G24Xc	N/A	12.1.1.4	1.0.3.7
S-G8Xc	N/A	12.1.1.4	1.0.3.7
10G4Xa	N/A	11.6.1.9	1.0.1.11
10G4Ca	N/A	12.0.1.11	1.0.1.11
10G4Xc	N/A	12.1.1.4	1.0.3.7
10G8Xc	N/A	12.1.1.4	1.0.3.7
S-10G1Xc	N/A	12.1.1.4	1.0.3.7
S-10G2Xc	N/A	12.5.3.9	1.0.3.9
PSU Controller	N/A	11.1.1.9	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.1.1.9	N/A

Table 1: BlackDiamond 8800 Series of Switches Component Support (Continued)

BlackDiamond 8810 and BlackDiamond 8806 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
600/900 W AC PSU (Model # 41050/PS 2431) (BlackDiamond 8806 only)	N/A	11.6.1.9	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.3.2.6	N/A

NOTE

Upgrading the BootROM on a BlackDiamond 8810 or BlackDiamond 8806 switch is not automatic when software is upgraded. The user must be running the minimum required BootROM version or later. Use the install firmware command after upgrading the ExtremeXOS image to insure the BootROM is at the latest level.

BlackDiamond 10808 Switch Component Support

BlackDiamond 10808 components supported with ExtremeXOS 12.5, and the minimum ExtremeXOS version required by the chassis to support each component, include:

Table 2: BlackDiamond 10808 Component Support

BlackDiamond Component	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-1	bd10k-12.5.4.5-patch1-6.xos	10.1.0	1.0.1.5
MSM-1XL	bd10k-12.5.4.5-patch1-6.xos	10.1.0	1.0.1.5
10G2X	N/A	11.1.1	1.3.0.0
10G2H	N/A	11.2.0	1.3.0.0
10G6X	N/A	10.1.0	1.3.0.0
G20X	N/A	11.1.1	1.3.0.0
G60X	N/A	10.1.0	1.3.0.0
G60T	N/A	10.1.0	1.3.0.0
PSU Controller	N/A	10.1.0	N/A
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	10.1.0	N/A
1200 W DC PSU (Model # 60021 PS 2350)	N/A	11.3.2.6	N/A

Following are the part numbers for the BlackDiamond 10808 modules with the Rev. D ASIC:

Table 3: BlackDiamond 10808 I/O Modules with Part Numbers

I/O Module	8000 Level Part No.	9000 Level Part No.	Description	ExtremeXOS Required
G60T	804403-00, after Rev. 16	904015-00	BlackDiamond 10808 60-port 10/100/1000BASE-T RJ-45 Module	11.2.1.3
	804408-00, after Rev. 03	904015-10	BlackDiamond 10808 60-port 10/100/1000BASE-T RJ-45 Module	11.2.1.3
G60X	804402-00, after Rev. 16	904009-00/11	BlackDiamond 10808 60-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
	804404-00, after Rev. 03	904009-10	BlackDiamond 10808 60-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
G20X	804407-00, after Rev. 03	904020-10	BlackDiamond 10808 20-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
	804470-00, after Rev. 08	904020-00/11	BlackDiamond 10808 20-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
10G2X	804410-00, after Rev. 03	904032-10	BlackDiamond 10808 2-port 10GBASE-X XENPAK Module	11.2.1.3
	804471-00, after Rev. 11	904032-00/11	BlackDiamond 10808 2-port 10GBASE-X XENPAK Module	11.2.1.3
10G2H	804406-00, after Rev. 09	904027-00/11	BlackDiamond 10808 Hybrid Module (2-port 10GBASE-X XENPAK, 20-port 1000BASE-X SFP, 20-port 10/100/1000BASE-T RJ-45)	11.2.1.3
	804411-00, after Rev. 03	904027-10	BlackDiamond 10808 Hybrid Module (2-port 10GBASE-X XENPAK, 20-port 1000BASE-X SFP, 20-port 10/100/1000BASE-T RJ-45)	11.2.1.3
10G6X	804405-00, after Rev. 18	904016-00/11	BlackDiamond 10808 6-port 10GBASE-X XENPAK Module	11.2.1.3
	804409-00, after Rev. 03	904016-10	BlackDiamond 10808 6-port 10GBASE-X XENPAK Module	11.2.1.3

BlackDiamond 12800 Series Switches Component Support

BlackDiamond 12802, BlackDiamond 12804, BlackDiamond 12802 R-Series, and BlackDiamond 12804 R-Series components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the chassis to support each component, include:

Table 4: BlackDiamond 12800 Series Switches Component Support

BlackDiamond 12802/12804 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-5R (BlackDiamond 12804)	bd12k-12.5.4.5-patch1-6.xos	11.4.1.4	1.0.0.2
MSM-5 (BlackDiamond 12804)	bd12k-12.5.4.5-patch1-6.xos	11.4.1.4	1.0.0.2
MSM-5 (BlackDiamond 12802)	bd12k-12.5.4.5-patch1-6.xos	12.0.1.11	1.0.0.2
MSM-6R	bd12k-12.5.4.5-patch1-6.xos	12.0.2.25	1.0.1.8
MSM-5R (BlackDiamond 12802)	bd12K-12.5.4.5-patch1-6.xos	12.0.1.11	1.0.0.2
XM-2X	N/A	12.3.1	N/A
XM-2XR	N/A	11.4.1.4	N/A
XM-2HR	N/A	12.1.1.4	N/A

Table 4: BlackDiamond 12800 Series Switches Component Support (Continued)

BlackDiamond 12802/12804 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
GM-20XTR	N/A	11.4.1.4	N/A
GM-20XT	N/A	11.4.1.4	N/A
GM-20T	N/A	11.4.1.4	N/A
PSU Controller	N/A	11.4.1.4	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.4.1.4	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.4.1.4	N/A

BlackDiamond 20800 Series Switch Component Support

BlackDiamond 20800 series switch components supported with ExtremeXOS 12.5, and the firmware version required by the software to support each component, include:

Table 5: BlackDiamond 20800 Series Switch Component Support

BlackDiamond 20800 Components	ExtremeXOS Filenames	ExtremeXOS Required	Firmware Version Required with ExtremeXOS 12.5.3
GM-40X	N/A	12.3.2	
uC			2.9
FPGA: A			0.1.7
FPGA: P			0.0.6
FPGA: T1			0.0.11
FPGA: W1 & W2			0.0.d
BootROM			0.3.5
HM-2X24GA	N/A	12.5.1	
uC			2.9
FPGA: A			0.1.7
FPGA: P			0.0.6
FPGA: T1			0.0.5
FPGA: W1			0.0.4
FPGA: D1			0.0.b
BootROM			0.3.5
XM-8X	N/A	12.3.2	
uC			3.0
FPGA: A			0.1.7
FPGA: P			0.0.6
FPGA: D1 and D2 (manual upgrade)			0.0.b
FPGA: T1 & T2			0.0.11
FPGA: WH			0.0.9
BootROM			0.3.5
XFM-1 (shown as Fabric-1 through Fabric-5) (BlackDiamond 20808)	N/A	12.3.2	
uC			2.9
XFM-2 (shown as Fabric-1 through Fabric-5) (BlackDiamond 20804)	N/A	12.4.1	
uC			2.9

Table 5: BlackDiamond 20800 Series Switch Component Support (Continued)

BlackDiamond 20800 Components	ExtremeXOS Filenames	ExtremeXOS Required	Firmware Version Required with ExtremeXOS 12.5.3
MM Basic	bd20k-12.5.4.5-patch1-6.xos	12.3.2	
uC			2.9
FPGA: S			0.3.e
BootROM			0.2.1
PSUCTRL			3.0
Fan Tray (BlackDiamond 20808)	N/A	12.3.2	
uC (shown as “Revision”)			2.9
Fan Tray (BlackDiamond 20804)	N/A	12.4.1	
uC (shown as “Revision”)			2.9

NOTE

Use the `check firmware version` command to verify that all components on the BlackDiamond 20800 series switches (I/O modules, fans, and so on) are running the latest version of ExtremeXOS firmware. If the command output shows that one or more component is not running the latest firmware, use the `install firmware` command to update all down level components. Be sure to run the `show slot`, `show fans`, `show power`, and `show fabric` commands to verify that all components are installed and operational before attempting to upgrade or downgrade the switch firmware.

Summit X150 and X350 Component Support

Summit X150 and X350 series components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the switch to support each component, include:

Table 6: Summit X150 and X350 Component Support

Summit X150 and X350 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X150-24t	summitX-12.5.4.5-patch1-6.xos	12.0.2.25	1.0.3.1
Summit X150-48t	summitX-12.5.4.5-patch1-6.xos	12.0.2.25	1.0.3.1
Summit X150-24p	summitX-12.5.4.5-patch1-6.xos	12.0.2.25	1.0.3.1
Summit X350-24t	summitX-12.5.4.5-patch1-6.xos	12.0.3.16	1.0.3.1
Summit X350-48t	summitX-12.5.4.5-patch1-6.xos	12.0.3.16	1.0.3.1
XGM2-2xf (Summit X350 only)	summitX-12.5.4.5-patch1-6.xos	12.1.2	N/A
XGM2-2sf (Summit X350 only)	summitX-12.5.4.5-patch1-6.xos	12.2.1	N/A
XGM2-2bt (Summit X350 only)	summitX-12.5.4.5-patch1-6.xos	12.2.1	N/A

Summit X250e Component Support

Summit X250e components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the switch to support each component, include

Table 7: Summit X250e Component Support

Summit X250 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X250e-24p	summitX-12.5.4.5-patch1-6.xos	12.0.1.11	1.0.3.0
Summit X250e-48p	summitX-12.5.4.5-patch1-6.xos	12.0.1.11	1.0.3.0
Summit X250e-24t	summitX-12.5.4.5-patch1-6.xos	12.0.1.11	1.0.3.0
Summit X250e-48t	summitX-12.5.4.5-patch1-6.xos	12.0.1.11	1.0.3.0
Summit X250e-24x	summitX-12.5.4.5-patch1-6.xos	12.0.2.25	1.0.3.1
Summit X250e-24tDC	summitX-12.5.4.5-patch1-6.xos	12.0.3.16	1.0.3.1
Summit X250e-24xDC	summitX-12.5.4.5-patch1-6.xos	12.0.3.16	1.0.3.1
Summit X250e-48tDC	summitX-12.5.4.5-patch1-6.xos	12.0.3.16	1.0.3.1

Summit X450a and X450e Component Support

Summit X450a and X450e components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the switch to support each component, include:

Table 8: Summit X450a and X450e Component Support

Summit X450a and X450e Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X450a Series			
Summit X450a-48t	summitX-12.5.4.5-patch1-6.xos	11.5.1.4	1.0.2.2
Summit X450a-48tDC	summitX-12.5.4.5-patch1-6.xos	11.6.1.9	1.0.2.2
Summit X450a-24t	summitX-12.5.4.5-patch1-6.xos	11.5.1.4	1.0.2.2
Summit X450a-24tDC	summitX-12.5.4.5-patch1-6.xos	11.5.1.4	1.0.2.2
Summit X450a-24xDC	summitX-12.5.4.5-patch1-6.xos	11.6.1.9	1.0.2.2
Summit X450a-24x	summitX-12.5.4.5-patch1-6.xos	11.6.1.9	1.0.2.2
Summit X450e Series			
Summit X450e-24p	summitX-12.5.4.5-patch1-6.xos	11.5.1.4	1.0.2.2
Summit X450e-48p	summitX-12.5.4.5-patch1-6.xos	11.6.1.9	1.0.2.2
Summit X450e-24t	summitX-12.5.4.5-patch1-6.xos	12.5.1	1.0.5.6
Summit X450e-48t	summitX-12.5.4.5-patch1-6.xos	12.5.1	1.0.5.6
Option Cards			
XGM2-2xn (Summit X450a and X450e series only)	summitX-12.5.4.5-patch1-6.xos	11.5.1.4	N/A
XGM2-2xf (Summit X450a and X450e series only)	summitX-12.5.4.5-patch1-6.xos	11.5.1.4	N/A

Table 8: Summit X450a and X450e Component Support (Continued)

Summit X450a and X450e Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
XGM2-2sf (Summit X450a and X450e series only)	summitX-12.5.4.5-patch1-6.xos	12.2.1	N/A
XGM2-2bt (Summit X450a and X450e series only)	summitX-12.5.4.5-patch1-6.xos	12.2.1	N/A

Summit X460 Component Support

Summit X460 components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the chassis to support each component, include:

Table 9: Summit X460 Component Support

Summit X460 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X460-24x	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
Summit X460-24t	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
Summit X460-24p	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
Summit X460-48x	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
Summit X460-48t	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
Summit X460-48p	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
Option Cards and Stacking Modules			
XGM3-2sf	summitX-12.5.4.5-patch1-6.xos	12.5.1	N/A
SummitStack	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0
SummitStack-V80	summitX-12.5.4.5-patch1-6.xos	12.5.1	2.0.1.0

Summit X480 Component Support

Summit X480 components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the chassis to support each component, include:

Table 10: Summit X480 Component Support

Summit X480 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X480-24x	summitX-12.5.4.5-patch1-6.xos	12.4.1	2.0.0.9
Summit X480-48x	summitX-12.5.4.5-patch1-6.xos	12.4.1	2.0.0.9
Summit X480-48t	summitX-12.5.4.5-patch1-6.xos	12.4.1	2.0.0.9
VIM2-SummitStack	summitX-12.5.4.5-patch1-6.xos	12.4.1	N/A
VIM2-SummitStack-V80	summitX-12.5.4.5-patch1-6.xos	12.5.3	N/A
VIM2-SummitStack128	summitX-12.5.4.5-patch1-6.xos	12.4.1	N/A
VIM2-10G4X	summitX-12.5.4.5-patch1-6.xos	12.4.1	N/A

Summit X650 Component Support

Summit X650 components supported with ExtremeXOS 12.5, and the minimum BootROM version required by the chassis to support each component, include:

Table 11: Summit X650 Component Support

Summit X650 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X650-24x	summitX-12.5.4.5-patch1-6.xos	12.3.1	1.0.5.5
Summit X650-24t	summitX-12.5.4.5-patch1-6.xos	12.3.1	1.0.5.5
VIM1-SummitStack	summitX-12.5.4.5-patch1-6.xos	12.3.1	N/A
VIM1-10G8X	summitX-12.5.4.5-patch1-6.xos	12.3,.1	N/A
VIM1-SummitStack256	summitX-12.5.4.5-patch1-6.xos	12.4.1	N/A
VIM1-SummitStack512	summitX-12.5.4.5-patch1-6.xos	12.3.3	N/A

NOTE

Upgrading the BootROM on Summit family switches is not automatic when software is upgraded. The user must be running the minimum required BootROM version. Use the `download bootrom` command to download a BootROM image.

SFP (Mini-GBIC) Support

SFPs supported on the BlackDiamond 8810 and BlackDiamond 8806 switches with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 12: BlackDiamond 8800 Series of Switches SFP Support

SFP	ExtremeXOS Required
1000BASE-T SFP	11.1.1.9
SX SFP	11.1.1.9
LX SFP	11.1.1.9
ZX SFP	11.1.1.9
100FX/1000LX SFP	11.3.1.3
100FX SFP	11.4.3.4 or 11.5.2.10 (not supported in 11.5.1.4)
1000BX SFP	11.4.1.4
LX100 SFP	12.0.1.11
10/100/1000BASE-T Copper SFP	12.0.2.25

Table 13: BlackDiamond 8800 Series of Switches SFP+ Support

SFP	ExtremeXOS Required
ER SFP+	12.3.3
SR SFP+	12.3.1

Table 13: BlackDiamond 8800 Series of Switches SFP+ Support (Continued)

SFP	ExtremeXOS Required
LR SFP+	12.3.1
SFP+ twin coax cable	12.3.1

SFPs supported on the BlackDiamond 10808 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 14: BlackDiamond 10808 Switch SFP Support

SFP	ExtremeXOS Required
LX100 SFP	12.0.1.11
SX SFP	10.1.0
LX SFP	10.1.0
ZX SFP	10.1.0
1000BASE-T SFP	11.1.1.9
1000BX SFP	11.6.1.9

SFPs supported on the BlackDiamond 12804 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 15: BlackDiamond 12804 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	11.4.1.4
LX SFP	11.4.1.4
ZX SFP	11.4.1.4
1000BASE-T SFP	11.4.1.4
1000BX SFP	11.6.1.9
LX100 SFP	12.0.1.11
100FX/1000LX SFP	11.6.1.9

SFPs supported on the BlackDiamond 12802 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 16: BlackDiamond 12802 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	12.0.1.11
LX SFP	12.0.1.11
ZX SFP	12.0.1.11
1000BASE-T SFP	12.0.1.11
1000BX SFP	12.0.1.11
LX100 SFP	12.0.1.11
100FX/1000LX SFP	12.0.1.11

SFPs supported on the BlackDiamond 20800 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 17: BlackDiamond 20800 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	12.2
LX SFP	12.2
ZX SFP	12.2
LX100	12.2
BXU	12.2
BXD	12.2

SFPs supported on the Summit X150 series switches with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 18: Summit X150 Series Switches SFP Support

SFP	ExtremeXOS Required
100BASE-FX (P/N 10067)	12.0.2.25
100BASE-BX SFP	12.0.2.25
100BASE LX10 SFP	12.0.2.25
SX SFP	12.0.2.25
LX SFP	12.0.2.25
ZX SFP	12.0.2.25
LX100 SFP	12.0.2.25
1000BX SFP	12.0.2.25

SFPs supported on the Summit X250e switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 19: Summit X250e SFP Support

SFP	ExtremeXOS Required
SX SFP, ports 25 and 26	12.0.2.25
LX SFP, ports 25 and 26	12.0.2.25
ZX SFP, ports 25 and 26	12.0.2.25
LX100 SFP, ports 25 and 26	12.0.2.25
1000BX SFP, ports 25 and 26	12.0.2.25
100BASE FX SFP (P/N 10067), ports 1 through 26	12.0.2.25
100BASE BX SFP, ports 1 through 26	12.0.2.25
100BASE LX10 SFP, ports 1 through 26	12.0.2.25

SFPs supported on the Summit X350 series switches with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

NOTE

The XGM2-2sf ports are 10Gb SFP+ ports and do not support 1-Gb optics (PD4-739782255).

Table 20: Summit X350 Series Switches SFP/SFP+ (XGM2-2sf Option Card Required) Support

SFP	ExtremeXOS Required
SX SFP	12.0.3.16
LX SFP	12.0.3.16
ZX SFP	12.0.3.16
LX100 SFP	12.0.3.16
1000BX SFP	12.0.3.16
ER SFP+	12.3.3
SR SFP+	12.2.1
LR SFP+	12.2.1
SFP+ twin coax cables	12.2.1

SFPs supported on the Summit X450a switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

NOTE

The XGM2-2sf ports are 10-Gb SFP+ ports and do not support 1-Gb optics (PD4-739782255).

Table 21: Summit X450a Switch SFP/SFP+ (XGM2-2sf Option Card Required) Support

SFP	ExtremeXOS Required
10/100/1000BASE-T Copper SFP **Note**: Not supported on combo ports.	12.0.2.25
SX SFP	11.2.2.4
LX SFP	11.2.2.4
ZX SFP	11.2.2.4
ER SFP+	12.3.3
SR SFP+	12.2.1
LR SFP+	12.2.1
SFP+ twin coax cables	12.2.1
100FX SFP (P/N 10063) **Note**: Not supported on combo ports.	11.6.1.9

Table 21: Summit X450a Switch SFP/SFP+ (XGM2-2sf Option Card Required) Support

SFP	ExtremeXOS Required
100FX/1000LX SFP • Summit X450a-24x, ports 1 through 20 **Note**: Not supported on combo ports.	11.6.1.9
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X450e switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

NOTE

The XGM2-2sf ports are 10-Gb SFP+ ports and do not support 1-Gb optics (PD4-739782255).

Table 22: Summit X450e Switch SFP/SFP+ (XGM2-2sf Option Card Required) Support

SFP	ExtremeXOS Required
SX SFP	11.6.1.9
LX SFP	11.6.1.9
ZX SFP	11.6.1.9
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9
ER SFP+	12.3.3
SR SFP+	12.2.1
LR SFP+	12.2.1
SFP+ twin coax cables	12.2.1

SFPs supported on the Summit X460 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 23: Summit X460 SFP/SFP+ (XGM3-2sf Option Cared Required) Support

SFP	ExtremeXOS Required
1000BASE-SX SFP	12.5.1
1000BASE-LX SFP	12.5.1
1000BASE-ZX SFP	12.5.1
1000BASE-BX SFP BX-D	12.5.1
1000BASE-BX SFP BX-U	12.5.1
LX100 SFP	12.5.1
10/100/1000BASE-T SFP	12.5.1
100BASE-BX SFP BX-D	12.5.1
100BASE-BX SFP BX-U	12.5.1
100BASE-FX/1000BASE-LX SFP	12.5.1
10GBASE-ER SFP+	12.5.1

Table 23: Summit X460 SFP/SFP+ (XGM3-2sf Option Cared Required) Support (Continued)

SFP	ExtremeXOS Required
10GBASE-SR SFP+	12.5.1
10GBASE-LR SFP+	12.5.1
100BASE-FX SFP	12.5.1
100BASE-LX10 SFP	12.5.1
100BASE-FX SFP	12.5.1

SFPs supported on the Summit X480 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 24: Summit X480 SFP Support

SFP	ExtremeXOS Required
SX mini-GBIC	12.4.1
LX mini-GBIC	12.4.1
ZX mini-GBIC	12.4.1
1000BASE-BX mini-GBIC BX-D	12.4.1
1000BASE-BX mini-GBIC BX-U	12.4.1
100BASE-BX mini-GBIC BX-D	12.4.1
100BASE-BX mini-GBIC BX-U	12.4.1
100BASE LX10 mini-GBIC	12.4.1
100BASE FX mini-GBIC module	12.4.1
LX100 mini-GBIC module	12.4.1
100 FX/1000LX mini-GBIC, not supported on combo ports	12.4.1
100FX mini-GBIC module, not supported on combo ports	12.4.1
10/100/1000BASE-T mini-GBIC, not supported on combo ports	12.4.1

SFPs supported on the Summit X650 series switches with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 25: Summit X650 Series Switches SFP/SFP+ Support

SFP	ExtremeXOS Required
SR SFP+, ports 1 through 24, and ports 25 through 32 (for the VIM1-10G8X)	12.3.1
LR SFP+, ports 1-24 and 25-32 for VIM1-10G8X	12.3.1
SFP+ twin coax cable - 1-24 and 25-32 for VIM1-10G8X	12.3.1
10/100/1000BASE-T SFP+ Copper—1000 speed support only **Note:** Not supported on port 23 and 24	12.3.3
ER SFP+	12.3.3
1000BX SFP, not supported on ports 23, 24	12.2.1
1000SX SFP, not supported on ports 23, 24	12.2.1
1000LX SFP, not supported on ports 23, 24	12.2.1

Table 25: Summit X650 Series Switches SFP/SFP+ Support

SFP	ExtremeXOS Required
1000 BASE-T SFP, not supported on ports 23, 24	12.3.1
LX100 SFP, not supported on ports 23, 24	12.2.1
ZX SFP, not supported on ports 23, 24	12.2.1

XENPAK Module Support

XENPAK modules supported on the BlackDiamond 10808 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 26: BlackDiamond 10808 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.1.1.9
ER	11.1.1.9
SR	11.1.1.9
LX4	11.3.1.3
ZR	11.3.1.3
LW	11.4.1.4

XENPAK modules supported on the BlackDiamond 12804 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 27: BlackDiamond 12804 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.4.1.4
ER	11.4.1.4
SR	11.4.1.4
LX4	11.4.1.4
ZR	11.4.1.4
LW	11.4.1.4

XENPAK modules supported on the BlackDiamond 12802 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 28: BlackDiamond 12802 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	12.0.1.11
ER	12.0.1.11
SR	12.0.1.11
LX4	12.0.1.11
ZR	12.0.1.11
LW	12.0.1.11

XENPAK modules supported on the Summit X350 switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 29: Summit X350 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	12.0.3.16
LR	12.0.3.16
ER	12.0.3.16
LX4	12.0.3.16
ZR	12.0.3.16

XENPAK modules supported on the Summit X450a switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 30: Summit X450a Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.6.1.9
LR	11.6.1.9
ER	11.6.1.9
LX4	11.6.1.9
ZR	11.6.1.9
LW	11.6.1.9
CX4	12.0.1.11

XENPAK modules supported on the Summit X450e switch with ExtremeXOS 12.5, and the minimum ExtremeXOS version required, include:

Table 31: Summit X450e Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.5.1.4
LR	11.5.1.4
ER	11.5.1.4
LX4	11.5.1.4
ZR	11.5.1.4
CX4	12.0.1.11

NOTE

XENPAKs not supplied by Extreme Networks will show up as “Unsupported Optic Module” in the `show port x:y` information detail and `show port x:y configuration` command output.

XFP Module Support

XFP modules supported on the BlackDiamond 8800 series of switches with ExtremeXOS 12.5, the minimum ExtremeXOS version required include:

Table 32: BlackDiamond 8800 Series of Switches XFP Support

XFP Module	ExtremeXOS Required
SR	11.6.1.9
LR	11.6.1.9
ER	12.0.2.25
DWDM	12.1.2.17
ZR	12.1.2.17
Tunable DWDM	12.5.1

XFP modules supported on the BlackDiamond 20800 switch with ExtremeXOS 12.5, the minimum ExtremeXOS version required include:

Table 33: BlackDiamond 20800 Switch XFP Support

XFP Module	ExtremeXOS Required
SR	12.2
LR	12.2
ER	12.2
ZR	12.2
Tunable DWDM	12.5.1

XFP modules supported on the Summit X350 switch with ExtremeXOS 12.5, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 34: Summit X350 Switch XFP Support

XFP Module	ExtremeXOS Required
SR	12.0.3.16
LR	12.0.3.16
ER	12.0.3.16
DWDM	12.5.1
ZR	12.1.2.17

XFP modules supported on the Summit X450a and X450e series switch with ExtremeXOS 12.5, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 35: Summit X450a and X450e Series Switch XFP Support

XFP Module	ExtremeXOS Required
SR	11.5.1.4
LR	11.5.1.4
ER	12.0.2.25

Table 35: Summit X450a and X450e Series Switch XFP Support (Continued)

XFP Module	ExtremeXOS Required
DWDM	12.5.1
ZR	12.1.2.17

XFP modules supported on the Summit X480 series switch with ExtremeXOS 12.5, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 36: Summit X480 Series Switch XFP Support

XFP Module	ExtremeXOS Required
SR	12.4.1
LR	12.4.1
ER	12.4.1
ZR	12.4.1
DWDM	12.4.1
Tunable DWDM	12.5.1

Upgrading to ExtremeXOS

See “Software Upgrade and Boot Options” in the *ExtremeXOS Concepts Guide* for instructions on upgrading ExtremeXOS software. Following are miscellaneous hitless upgrade notes:

- Beginning with ExtremeXOS 12.1, an ExtremeXOS core image (.xos file) must be downloaded and installed on the alternate (non-active) partition. If you try to download to an active partition, the error message "Error: Image can only be installed to the non-active partition." is displayed. An ExtremeXOS modular software package (.xmod file) can still be downloaded and installed on either the active or alternate partition.
- For the BlackDiamond 8800 series of switches, a hitless upgrade to ExtremeXOS 12.5.2 from an earlier release is not supported and should not be attempted. Use the normal software upgrade process for these switches.
- Hitless upgrade from ExtremeXOS 12.0 and earlier to ExtremeXOS 12.1 and later is not supported on the BlackDiamond 12800 switch.

Downloading Supported MIBs

The Extreme Networks MIBs are located on the eSupport website under Download Software Updates, located at:

https://esupport.extremenetworks.com/

ExtremeXOS Command Line Support

The following is true for all Summit X150 and X350 series switches:

- Summit X150 and X350 series switches do not support L3 functionality; this platform does not support CLI commands for L3 functionality.
- Summit X150 and X350 series switches do not support stacking; all CLI commands for stacking are not supported on this platform.
- Summit X150 and X350 series switches do not support IP forwarding; however, CLI commands that configure IP addresses function in order to access the management functionality of the switch are supported.
- Upgrade or trial licensing is not available on the Summit X150 and X350 series switches.

Tested Third-Party Products

This section lists the third-party products tested for ExtremeXOS 12.6.2.

Tested RADIUS Servers

The following RADIUS servers are fully tested:

- Microsoft—Internet Authentication Server
- Funk Software—Steel-Belted RADIUS Enterprise Edition 4.5

- Meetinghouse
- FreeRADIUS

Tested Third-Party Clients

The following third-party clients are fully tested:

- Funk Odyssey 2.2
- MeetingHouse Data AEGIS 2.0.5
- Odyssey 3.03.0.1194

PoE Capable VoIP Phones

The following PoE capable VoIP phones are fully tested:

- Avaya 4620
- Avaya 4620SW IP telephone
- Avaya 9620
- Avaya 4602
- Avaya 9630
- Avaya 4621SW
- Avaya 4610
- Avaya 1616
- Avaya one-X
- Cisco 7970
- Cisco 7910
- Cisco 7960
- ShoreTel ShorePhone IP 212k
- ShoreTel ShorePhone IP 560
- ShoreTel ShorePhone IP 560g
- ShoreTel ShorePhone IP 8000
- ShoreTel ShorePhone IP BB 24
- Siemens OptiPoint 410 standard–2
- Siemens OpenStage 20
- Siemens OpenStage 40
- Siemens OpenStage 60
- Siemens OpenStage 80

Extreme Switch Security Assessment

DoS Attack Assessment

Tools used to assess DoS attack vulnerability:

- Network Mapper (NMAP)

ICMP Attack Assessment

Tools used to assess ICMP attack vulnerability:

- SSPing
- Twinge
- Nuke
- WinFreeze

Port Scan Assessment

Tools used to assess port scan assessment:

- Nessus

2 CHAPTER Limits

This chapter summarizes the supported limits in ExtremeXOS 12.6.2.

Supported Limits

Table 37 summarizes tested metrics for a variety of features, as measured in a per-system basis unless otherwise noted. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeXOS Concepts Guide*.

NOTE

The term “BlackDiamond 8000 e-series” refers to all BlackDiamond 8500 e-series and 8800 e-series modules.The term “BlackDiamond 8000 series” refers to all BlackDiamond 8500, 8800, and 8900 series modules.

The scaling and performance information shown in Table 37 is provided for the purpose of assisting with network design. It is recommended that network architects and administrators design and manage networks with an appropriate level of network scaling “head room.” The scaling and performance figures provided have been verified using specific network topologies using limited switch configurations. There is no guarantee that the scaling and performance figures shown are applicable to all network topologies and switch configurations and are provided as a realistic estimation only. If you experience scaling and performance characteristics that you feel are sufficiently below what has been documented, contact Extreme Networks technical support for additional assistance.

The route limits shown in Table 37 for IPv4 and IPv6 routing protocols are software limits only. The actual hardware limits may be lower than the software limits, based on platform. The hardware limits for specific platforms are specified as "IPv4/IPv6 routes (LPM entries in hardware)" in the following table.

On certain BlackDiamond 8000 and Summit products, it is not advised to have greater than 25,000 total IP routes from all routing protocols. This includes a BlackDiamond 8000 series switch with an 8500-MSM24, MSM-G8X or MSM-48, and Summit X250e, X450a, X450e, X650 or X670 switches, either in a SummitStack or standalone. Adverse effects can occur with routing tables larger than this, especially when a single network event or CLI command affects a significant number of routes. For example, just after such a network event, the added system load will cause a “save configuration” command to time out.

Table 37: Supported Limits

Metric	Product	Limit
Access lists (meters)—maximum number of meters,	BlackDiamond 8000 series	
	e-series, group of 24 ports	512
	a-series, group of 24 ports	1,024
	c-series	2,048 ingress, 256 egress
	BlackDiamond 8900 series	
	8900-10G24X-c, group of 12 ports	1,024 ingress, 256 egress
	8900 xl-series, 8900-G96T-c	4,096 ingress, 512 egress
	8900-40G6X-xm	512 ingress 256 egress
	Summit X150, X250e, X350, X450e group of 24 ports	512
	Summit X450a, group of 24 ports	1,024
	Summit X460 group of 24 ports	2,048 ingress, 256 egress
	Summit X480	4,096 ingress, 512 egress
	Summit 650, group of 12 ports	1,024 ingress, 256 egress
	VIM3-40G-4x	512 ingress 256 egress
	Summit X670	
	VIM4-40G4x	512 ingress 256 egress
Access lists (policies)—suggested maximum number of lines in a single policy file.	All platforms	300,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Access lists (policies)—maximum number of rules in a single policy file.[a]	BlackDiamond 8000 series	
	a-series, group of 24 ports	2,048
	c-series, group of 24 ports	4,096 ingress, 512 egress
	e-series, group of 24 ports	1,024 ingress
	BlackDiamond 8900 c-series	
	8900-10G24X-c modules, group of 12 ports	2,048 ingress, 512 egress
	8900-G96T-c modules, group of 48 ports	8,192 ingress, 1,024 egress
	8900 xl-series	61,440 (up to)
	8900-40G6X-xm	2,048 ingress, 1,024 egress
	BlackDiamond 10808	30,000
	Summit X150, X250e, X350, X450e group of 24 ports	1,024
	Summit X450a, group of 24 ports	2,048
	Summit 460	4,096 ingress, 512 egress
	Summit X480	61,440 (up to) ingress[b], 1,024 egress
	Summit X650, group of 12 ports	2,048 ingress, 512 egress
	VIM3-40G4x	2,048 ingress, 1,024 egress
	Summit X670	2,048 ingress 1,024 egress
	VIM4-40G4x	

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Access lists (slices)—number of ACL slices.	BlackDiamond 8000 series	
	a- and c-series, group of 48 ports	16
	e-series, group of 24 ports	8
	BlackDiamond 8900 series	
	8900-10G24X-c modules, group of 12 ports	12 ingress, 4 egress
	8900-G96T-c modules, group of 48 ports	16 ingress, 4 egress
	8900 xl-series	17[b]
	8900-40G6X-xm	10 ingress, 4 egress
	Summit X150, X250e, X350, X450e, group of 48 ports	8
	Summit X450a, group of 24 ports	16
	Summit 460	16 ingress, 4 egress
	Summit X480	17[b] ingress, 4 egress
	Summit X650, group of 12 ports	12 ingress, 4 egress
	VIM3-40G4x	10 ingress, 4 egress
	Summit X670	10 ingress, 4 egress
	VIM4-40G4x	
ACL static ingress L2 entries—maximum number of static ACL L2 entries.	BlackDiamond 12800 series	10,000
	BlackDiamond 20800 series	10,000
ACL static ingress L3 rules—maximum number of static L3 ACL rules.	BlackDiamond 12800 series	20,000
	BlackDiamond 20800 series	20,000
ACL static egress L2 entries—maximum number of static ACL L2 entries.	BlackDiamond 12800 series	20,000
	BlackDiamond 20800 series	20,000
ACL static egress L3 rules—maximum number of static L3 ACL rules.	BlackDiamond 12800 series	20,000
	BlackDiamond 20800 series	20,000
ACL dynamic L2 entries—maximum number of ACL L2 entries	BlackDiamond 20800 series	2,000
ACL dynamic L3 rules—maximum number of L3 ACL rules	BlackDiamond 20800 series	2,000
AAA (local)—maximum number of admin and local user accounts.	All platforms	16
BFD (bidirectional forwarding detection)—maximum BFD sessions with MPLS as client.	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
	BlackDiamond 20800 series	64
	Summit X460	32
	Summit X480	32
	Summit X670	32

Table 37: Supported Limits (Continued)

Metric	Product	Limit
BFD sessions—maximum BFD sessions with static route as client.	All platforms (default timers)	512
	All platforms (minimal timers)	10
BGP (aggregates)—maximum number of BGP aggregates.	All platforms with Core license or higher	256
BGP (networks)—maximum number of BGP networks.	All platforms (except BlackDiamond 20800 series) with Core license or higher	1,024
	BlackDiamond 20800 series	2,048
BGP (peers)—maximum number of BGP peers.	BlackDiamond 8000 series	256*
	BlackDiamond xl-series	512
	BlackDiamond 10808	
	MSM-1XL MSM-1	512 256
	BlackDiamond 12800 series	
	MSM-5, MSM-5R MSM-6R	256* 512
	BlackDiamond 20800 series	512
	Summit X450a, X460, X650, X670	128*
	Summit X480	512
	* With default keepalive and hold timers.	
BGP (peer groups)—maximum number of BGP peer groups.	All platforms (except BlackDiamond 8900 series, BlackDiamond 20800 series, and Summit X480) with Core license or higher	64
	BlackDiamond 8900 series	128
	BlackDiamond 20808 series	128
	Summit X480	128
BGP (policy entries)—maximum number of BGP policy entries per route policy.	All platforms with Core license or higher	256
BGP (policy statements)—maximum number of BGP policy statements per route policy.	All platforms with Core license or higher	1,024
BGP (unicast address-family routes)—maximum number of unicast address-family routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8000 series	25,000
	BlackDiamond 8900 xl-series	524,256 (up to)[b]
	BlackDiamond 10808	
	MSM-1XL MSM-1	1,000,000 400,000
	BlackDiamond 12800 series	
	MSM-5, MSM-5R MSM-6R	400,000 1,000,000
	BlackDiamond 20800 series	512,000
	Summit X450a, X460, X650, X670	25,000
	Summit X480	524,256 (up to)[b]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
BGP (non-unique routes)—maximum number of non-unique BGP routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8000 series	25,000
	BlackDiamond 8900 xl-series	1,000,000
	BlackDiamond 10808	
	MSM-1XL MSM-1	2,000,000 900,000
	BlackDiamond 12800 series	
	MSM-5, MSM-5R MSM-6R	900,000 2,000,000
	BlackDiamond 20800 series	2,000,000
	Summit X450a, X460, X650, X670	25,000
	Summit X480	1,000,000
BGP multicast address-family routes — maximum number of multicast address-family routes.	BlackDiamond 8000 series	25,000
	BlackDiamond 8900 xl-series	524,256 (up to)[b]
	BlackDiamond 10808	
	MSM-1XL MSM-1	1,000,000 450,000
	BlackDiamond 12800 series	
	MSM-5, MSM-5R MSM-6R	450,000 1,000,000
	BlackDiamond 20800 series	512,000
	Summit X450a, X460, X650, X670	25,000
	Summit X480	524,256 (up to)[b]
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per virtual router.	All platforms	4
CLEAR-Flow—total number of rules supported. The ACL rules plus CLEAR-Flow rules must be less than the total number of supported ACLs. **Note:** CLEAR-Flow is not supported on "e" series switches and is only supported in a non-stack configuration in the Summit family of switches.	BlackDiamond 8800 c-series	4,096
	BlackDiamond 8900 series	4,096
	BlackDiamond 20800 series	5,000
	Summit X450a, X650, X670	2,048
	Summit X480	4,096
Connectivity Fault Management (CFM)—maximum number or CFM domains.	All platforms	8
CFM—maximum number of CFM associations.	All platforms	4,094
CFM—maximum number of CFM up end points.	BlackDiamond 8000 series	32
	BlackDiamond 10808	1,000
	BlackDiamond 12800 series	1,000
	BlackDiamond 20800 series	1,000
	Summit series	32

Table 37: Supported Limits (Continued)

Metric	Product	Limit
CFM—maximum number of CFM down end points.	BlackDiamond 8000 series	32
	BlackDiamond 10808	1,000
	BlackDiamond 12800 series	1,000
	BlackDiamond 20800 series	1,000
	Summit series	32
CFM—maximum number of CFM remote end points per up/down end point.	All platforms	64
CFM—maximum number of dot1ag ports.	All platforms	128
CFM—maximum number of CFM segments.	All platforms	1,000
Data Center Bridging eXchange (DCBX) protocol Type Length Value (TLVs)—maximum number of DCBX application TLVs.	All platforms	8
Dynamic ACLs—maximum number of ACLs processed per second. **Note**: Limits are load dependent.	BlackDiamond 8800 with c-series MSM and I/O modules	8
	BlackDiamond 8900 series	8
	BlackDiamond 12800 series	12
	Summit X450a, X480, X650, X670	
	with 50 DACLs with 500 DACLs	10 5
EAPS domains—maximum number of EAPS domains. **Note**: An EAPS ring that is being spatially reused cannot have more than four configured EAPS domains.	BlackDiamond 8000 series	64
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	BlackDIamond 20800 series	128
	Summit series	32
EAPSv1 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8000 series	2,000
	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
	BlackDiamond 20800 series	4,000
	Summit series	1,000
EAPSv2 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8000 series	2,000
	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
	BlackDIamond 20800 series	4,000
	Summit series	500
ELSM (vlan-ports)—maximum number of VLAN ports.	BlackDiamond 8000 series	5,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	BlackDIamond 20800 series	5,000
	Summit series	5,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
ESRP groups—maximum number of ESRP groups.	All platforms	7
ESRP domains—maximum number of ESRP domains.	BlackDiamond 8000 series	64
	BlackDiamond 8900 series	128
	BlackDiamond 10808	128
	BlackDiamond 12800 series	64
	BlackDiamond 20800 series	128
	Summit series	64
ESRP VLANs—maximum number of ESRP VLANs.	BlackDiamond 8000 series	1,000
	BlackDiamond 8900 series	2,048
	BlackDiamond 10808	3,000
	BlackDiamond 12800 series	3,000
	BlackDiamond 20800 series	255
	Summit series	1,000
ESRP (maximum ping tracks)—maximum number of ping tracks per VLAN.	All platforms	8
ESRP (IP route tracks)—maximum IP route tracks per VLAN.	All platforms	8
ESRP (VLAN tracks)—maximum number of VLAN tracks per VLAN.	All platforms	1
Forwarding rate—maximum L2/L3 software forwarding rate.	BlackDiamond 8000 series	10,000 pps
	BlackDiamond 12800 series	16,000 pps
	Summit series	10,000 pps
FDB (blackhole entries)—maximum number of unicast blackhole FDB entries.	BlackDiamond 8800 a-series	16,000
	BlackDiamond 8800 c-series	32,000
	BlackDiamond 8000 e-series	8,000
	Black Diamond 8900 series	BlackDiamomd
	8900 c-series 8900 xl-series 8900-40G6X-xm	32,000 524,288 (up to)[b] 128,000
	BlackDiamond 20800 series	100,000
	Summit X150, X250e, X350, X450e	8,000
	Summit X450a	16,000
	Summit X480	524,288 (up to)[b]
	Summit X 460	32,000
	Summit X650	
	VIM3-40G4x	32,000
	Summit X670	
	VIM4-40G4x	128,000
FDB (blackhole entries)—maximum number of multicast blackhole FDB entries.	BlackDiamond 8000 series	1,024
	Summit series	1,024
FDB (MAC learning rate)—maximum number of packets per second.	BlackDiamond 20800 series	200,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
FDB (maximum L2/L3 entries)—maximum number of MAC addresses/IP host routes.	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
FDB (maximum L2 entries)—maximum number of MAC addresses.	BlackDiamond 8800 a-series	16,384
	BlackDiamond 8000 c-series	32,768
	BlackDiamond 8000 e-series	8,192
	BlackDiamond 8000 (system), except 8900 xl-series	128,000
	BlackDiamond 8900 xl-series	524,488 (up to)[b]
	BlackDiamond 20800 series	400,000
	Basic I/O modules Advanced I/O modules	512,000 1,049,000
	Summit X150, X350, X250e, X450e	8,192
	Summit X450a	16,384
	Summit X480	524,488 (up to)[b]
	Summit X460, 650	32,768
	SummitStack, except X480	128,000
	Summit X670	131,072
Hierarchical QoS—maximum number of ingress-only traffic queues per system. (For 20XTR, first 10 ports ranges from 1 to 10 are UNIT-I, second 10 ports ranges from 11 to 20 are UNIT-II, for 10 Gig slot each port is one UNIT.)	BlackDiamond 12800 R-series	20,000
Hierarchical QoS—maximum number of ingress traffic queues with egress shaping allowed per switch.	BlackDiamond 12800 R-series	20,000
Hierarchical QoS—maximum number of egress-only traffic queues allowed per switch.	BlackDiamond 12800 R-series	20,000
Hierarchical QoS—maximum number of traffic queues attach per port.	BlackDiamond 12800 R-series	4,076
	BlackDiamond 20800 series (This is based on traffic queue mode [strict priority/ bandwidth]. This number will decrease the more egress ports are configured.)	1,142/824
Identity management—-—maximum number of roles that can be created.	All platforms except BlackDiamond 20800 series	64
Identity management—-maximum role hierarchy depth allowed.	All platforms except BlackDiamond 20800 series	5
Identity management—-maximum number of attribute value pairs in a role match criteria.	All platforms except BlackDiamond 20800 series	16
Identity management—-maximum of child roles for a role.	All platforms except BlackDiamond 20800 series	8
Identity management—-maximum number of policies/dynamic ACLs that can be configured per role.	All platforms except BlackDiamond 20800 series	8

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Identity management—-maximum number of LDAP servers that can be configured.	All platforms except BlackDiamond 20800 series	8
Identity management—-maximum number of kerberos servers that can be configured.	All platforms except BlackDiamond 20800 series	20
Identity management—-maximum database memory-size.	All platforms except BlackDiamond 20800 series	64–49,152
Identity management—-recommended number of identities per switch. **Note:** Number of identities per switch is for a default identity management database size (512 Kbytes) across all platforms.	All platforms except BlackDiamond 20800 series	100
Identity management—-recommended number of ACL entries per identity. **Note:** Number of ACLs per identity based on system ACL limitation.	All platforms except BlackDiamond 20800 series	20
Identity management—-maximum number of dynamic ACL entries configured as an individual dynamic rule, or as an ACL entry in a policy file.	All platforms except BlackDiamond 20800 series	500
IGMP sender—maximum number of IGMP senders per switch (IP multicast compression disabled).	BlackDiamond 8800 a-series	1,024
	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 8000 e-series	500[d]
	8900-10G24X-c modules	2,048[c]
	8900-G96T-c modules	4,096[c]
	8900-40G6X-xm	3,000[d]
	8900 xl-series	4,096[c]
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	BlackDiamond 20800 series	3,700
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	1,024
	Summit X480	4,096
	Summit X460	2,048
	Summit X650	2,048
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IGMP sender—maximum number of IGMP senders per switch (IP multicast compression enabled).	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 c-series	6,000[d]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 c-series	6,000[d]
	BlackDiamond 8900 xl-series	12,000[b]
	8900-40G6X-xm	3,000[d]
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	2,000[d]
	Summit X460	6,000[d]
	Summit X480	12,000[b]
	Summit X650	6,000[d]
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]
IGMP snooping per VLAN filters—maximum number of VLANs supported in per-VLAN IGMP snooping mode.	BlackDiamond 8800 a-series	1,000
	BlackDiamond 8800 c-series	2,000
	BlackDiamond 8000 e-series	448
	BlackDiamond 8900 c-series	1,000
	BlackDiamond 8900 xl-series	4,000
	8900-40G6X-xm	1,000
	Summit X150, X250e, X350, X450e	448
	Summit X450a, X460, X650, X670	1,000
	Summit X480	4,000
IGMPv1/v2 SSM-map entries—maximum number of IGMPv1/v2 SSM mapping entries.	All platforms	500
IGMPv1/v2 SSM-MAP entries—maximum number of sources per group in IGMPv1/v2 SSM mapping entries.	All platforms	50
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per port.	BBlackDiamond 8800 c-series	2,000
	BlackDiamond 8900 c-series	2,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	BlackDIamond 20800 series	5,000
	Summit series (except Summit X480, X650, and X670)	1,000
	Summit X460, X480, X650, X670	2,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per switch.	BlackDiamond 8800 c-series	20,000
	BlackDiamond 8900 c-series	20,000
	BlackDiamond 10808	30,000
	BlackDiamond 12800 series	30,000
	BlackDiamond 20800 series	30,000
	Summit series (except Summit X480, X650, and X670)	10,000
	Summit X460, X480, X650, X670	20,000
IGMPv3 maximum source per group—maximum number of source addresses per group.	All platforms	250
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per port.	BlackDiamond 8800 a-, e-series	1,000
	BlackDiamond 8800 c-series	2,000
	BlackDiamond 8900 series	5,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	BlackDiamond 20800 series	5,000
	Summit series (except Summit X460)	1,000
	Summit X460	2,000
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per switch.	BlackDiamond 8800 a-, e-series	10,000
	BlackDiamond 8800 c-series	20,000
	BlackDiamond 8900 series	30,000
	BlackDiamond 10808	30,000
	BlackDiamond 12800 series	30,000
	BlackDiamond 20800 series	30,000
	Summit series (except Summit X460)	10,000
	Summit X460	20,000
IP ARP entries in software—maximum number of IP ARP entries in software.	All platforms (except BlackDiamond 20800 series)	20,480
	BlackDiamond 20800 series	32,000
IP ARP entries in software with distributed mode on—maximum number of IP ARP entries in software with distributed mode on.	BlackDiamond 8000 series with 8900-MSM128 or MSM-48c, and only 8900 xl-series I/O modules	260,000
	BlackDiamond 8000 series with any I/O modules that are not 8900 xl-series	100,000
	All other platforms	8,000
		N/A

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IPv4 ARP entries in hardware with distributed mode on—maximum number of IP ARP entries in hardware with distributed mode on	Per BlackDiamond 8900-10G8X-xl, up to 260,000 per system	32,500[b]
	Per BlackDiamond 8900-G48X-xl or 8900-G48T-xl, up to 130,000 per system	16,250[b]
	Per BlackDiamond 8000 c-series, up to 18,000 per system	8,000
	BlackDiamond 8900-40G6X-xm, up to 22,000 per system	8,000
	All other platforms	N/A
IPv4 ARP entries in hardware with minimum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with minimum LPM routes present. For BlackDiamond 8800 and Summit series switches, assumes number of IP route reserved entries is 100 or less.	BlackDiamond 8800 a-, c-, xm-series	8,000
	BlackDiamond 8000 e-series	1,000[d]
	BlackDiamond 8900 xl-series	16,000
	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
	BlackDiamond 20800 series	32,000
	Summit X250e, X450e	1,000[d]
	Summit X450a, X650, X670	8,000
	Summit X460, X480	16,000
IPv4 ARP entries in hardware with maximum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with maximum LPM routes present. For BlackDiamond 8800 and Summit series, assumes number of IP route reserved entries is "maximum."	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 c-, xm-series	6,000[d]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 xl-series	12,000[d]
	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
	BlackDiamond 20800 series	32,000
	Summit X250e, X450e	500[d]
	Summit X450a	2,000[d]
	Summit X460, X480	12,000[d]
	Summit X650, X670	6,000[d]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IPv4 remote hosts in hardware with zero LPM routes—maximum recommended number of IPv4 remote hosts (hosts reachable through a gateway) in hardware when LPM routing is not used. For BlackDiamond 8800 and Summit series, assumes number of IP route reserved entries is 0, and number of IPv4 ARP entries present is 100 or less.	BlackDiamond 8800 a-series	14,000[d]
	BlackDiamond 8800 c-series	18,000[d]
	BlackDiamond 8000 e-series	1,000[d]
	BlackDIamond 8900 xl-series	40,000[b]
	BlackDiamond 8900-40G6X-xm	22,000[d]
	BlackDiamond 10808	N/A
	BlackDiamond 12800 series	N/A
	BlackDiamond 12800 R-series	N/A
	BlackDiamond 20800 series	N/A
	Summit X250e, X450e	1,000[d]
	Summit X450a	14,000[d]
	Summit X460	20,000[d]
	Summit X480	40,000[b]
	Summit X650	18,000[d]
	Summit X670	22,000[d]
IPv4 routes—maximum number of IPv4 routes in software (combination of unicast and multicast routes).	BlackDiamond 8900 xl-series with 8900-MSM128 or MSM-48c	524,256 (up to)[b]
	All other BlackDiamond 8000 series hardware	25,000
	BlackDiamond 10808	1,000,000
	BlackDiamond 12800 series	1,000,000
	BlackDiamond 20800 series	1,000,000
	Summit X250e, X450a, X450e, X460, X650, X670	25,000
	SummitStack or standalone	
	Summit X480	524,256 (up to)[b]
	SummitStack or standalone	
IPv4 routes (LPM entries in hardware)—number of IPv4 routes in hardware.	BlackDiamond 8800 a-, c-series	12,000
	BlackDiamond 8000 e-series	480
	BlackDiamond 8900 xl-series	524,256 (up to)[b]
	BlackDiamond 8900-40G6X-xm	16,000
	BlackDiamond 10808	256,000
	MSM-1 MSM-1XL	98,000 229,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R, MSM-6R	49,000 229,000
	BlackDiamond 20800 series	512,000
	Summit X250e, X450e	480
	Summit X450a, X460, X650	12,000
	Summit X480	524,256 (up to)[b]
	Summit X670	16,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IPv6 addresses on an interface—maximum number of IPv6 addresses on an interface.	All platforms	255
IPv6 addresses on a switch—maximum number of IPv6 addresses on a switch	BlackDiamond 8000 series	512
	BlackDiamond 10808	1,024
	BlackDiamond 12800 series	1,024
	BlackDiamond 20800 series	1,024
	Summit X460, X480, X650, X670	512
IPv6 host entries in hardware—maximum number of IPv6 neighbor entries in hardware.	BlackDiamond 8800 a-series	1,000[d]
	BlackDiamond 8800 c-, xm-series	3,000[d]
	BlackDiamond 8000 e-series	250[d]
	BlackDiamond 8900-10G24X-c modules	2,000[d]
	BlackDiamond 8900-G96T-c modules	4,000[d]
	BlackDiamond 8900 xl-series	4,000[d]
	BlackDiamond 10808	112,000
	BlackDiamond 12800 series	24,500
	BlackDiamond 12800 R-series	112,000
	BlackDiamond 20800 series	40,000
	Summit X250e, X450e	250[d]
	Summit X450a	1,000[d]
	Summit X460, X670	3,000[d]
	Summit X650	2,000[d]
IPv6 routes (LPM entries in hardware)—maximum number of IPv6 routes in hardware.	BlackDiamond 8800 a-, c-series	6,000
	BlackDiamond 8000 e-series	240
	BlackDiamond 8900 xl-, xm-series	8,000
	BlackDiamond 10808	114,500
	BlackDiamond 12800 series	114,500
	BlackDiamond 20800 series	40,000
	Summit X250e, X450e	240
	Summit X450a, X460, X650	6,000
	Summit X480, X670	8,000
IPv6 routes with a mask greater than 64 bits in hardware—maximum number of such IPv6 LPM routes in hardware.	BlackDiamond 8000 a-, c-, e-, xl-, xm-series	256
	BlackDiamond 10808	114,500
	BlackDiamond 12800 series	114,500
	BlackDiamond 20800 series	40,000
	Summit X250e, X450e, X450a, X460, X480, X650, X670	256

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IPv6 routes in software—maximum number of IPv6 routes in software.	BlackDiamond 8900 xl-series with 8900-MSM128 or MSM-48c	65,000
	All other BlackDiamond 8000 series hardware	25,000
	BlackDiamond 10808	65,000
	BlackDiamond 12800 series	65,000
	BlackDiamond 20800 series	65,000
	Summit X250e, X450a, X450e, X460, X650, X670	25,000
	Summit X480, SummitStack, or standalone	65,000
IP router interfaces—maximum number of VLANs performing IP routing–excludes sub VLANs (IPv4 and IPv6 interfaces).	All BlackDiamond 8000 series and Summit family switches with Edge license or higher	512
	All other BlackDiamond platforms	4,096
IP multicast static routes—maximum number of permanent multicast IP routes.	All platforms	1,024
IP unicast static routes—maximum number of permanent IP unicast routes.	All platforms	1,024
IP route sharing (maximum gateways)—configurable maximum number of configurable gateways used by equal cost multipath OSPF, BGP, or static routes.	BlackDiamond 8000 series	2, 4, or 8
	Summit series	2, 4, or 8
IP route sharing (total destinations)—maximum number of unique destinations used by multipath OSPF, OSPFv3, BGP, IS-IS, or static routes. OSPFv3 only applies to BlackDiamond 10808 and BlackDiamond 12800 series, which support ECMP for IPv6.	BlackDiamond 8800 a-series, c-series	
	with up to 8 gateways per destination	12,256
	BlackDiamond 8000 e-series	
	with up to 8 gateways per destination	480
	BlackDiamond 8900 xl-series	
	with up to 8 gateways per destination	524,256 (up to)[b]
	BlackDiamond 8900-40G6X-xm	
	with up to 8 gateways per destination	16,352
	BlackDiamond 10808	
	with up to 8 gateways per destination	7,136
	BlackDiamond 12800 series	
	with up to 8 gateways per destination	7,136
	BlackDiamond 20800 series	
	with up to 8 gateways per destination	512,000
	Summit X250e, X450e	
	with up to 8 gateways per destination	480
	Summit X450a, X460, X650	
	with up to 8 gateways per destination	12.256
	Summit X480	
	with up to 8 gateways per destination	524,256 (up to)[b]
	Summit X670	
	with up to 8 gateways per destination	16,352

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IP route sharing (total combinations of gateway sets)—maximum number of combinations of sets of adjacent gateways used by multipath OSPF, BGP, IS-IS, or static routes.	BlackDiamond 8800 a-series	
	default maximum gateways of 4 if maximum gateways is 2 if maximum gateways is 8	510 1,022 254
	BlackDiamond 8000 e-series	
	default maximum gateways of 4 if maximum gateways is 2 if maximum gateways is 8	30 62 14
	BlackDiamond 8800 c-, xl-, xm-series	
	default maximum gateways of 4 if maximum gateways is 2 if maximum gateways is 8	510 1,022 254
	BlackDiamond 20800 series	
	with up to 8 gateways per set	60
	Summit X460, X480, X650, X670	
	default maximum gateways of 4 if maximum gateways is 2 if maximum gateways is 8	510 1,022 254
IP multinetting (secondary IP addresses)—maximum number of secondary IP addresses per VLAN.	All platforms	64
IS-IS adjacencies—maximum number of supported IS-IS adjacencies.	BlackDiamond 8000 series	128
	BlackDiamond 8900 xl-series	255
	BlackDiamond 10808	255
	BlackDiamond 12800 series	255
	BlackDiamond 20800 series	255
	Summit X450a, X460, X480, X650, X670	128
IS-IS ECMP—maximum number of equal cost multipath for IS-IS.	BlackDiamond 8000 series	2, 4, or 8
	BlackDiamond 10808	8
	BlackDiamond 12800 series	8
	BlackDiamond 20800 series	8
	All Summit series	2, 4, or 8
IS-IS interfaces—maximum number of interfaces that can support IS-IS.	All platforms	255
IS-IS routers in an area—recommended maximum number of IS-IS routers in an area.	Summit X480	128
	All other platforms	256
IS-IS route origination—recommended maximum number of routes that can be originated by an IS-IS node.	BlackDiamond 8000 series	20,000
	BlackDiamond 8900 xl-series	30,000
	BlackDiamond 10808	30,000
	BlackDiamond 12800 series	30,000
	BlackDiamond 20800 series	30,000
	Summit X450a	5,000
	SUmmit X480	30,000
	Summit X460, X650, X670	20,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IS-IS IPv4 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router.	BlackDiamond 8000 series	25,000
	BlackDiamond 8900 xl-series	120,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	120,000 180,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	100,000 120,000 180,000
	BlackDiamond 20800 series	120,000
	Summit X450a	5,000
	Summit X480	50,000
	Summit X460, X650, X670	25,000
IS-IS IPv4 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8000 series	25,000
	BlackDiamond 8900 xl-series	120,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	120,000 180,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	100,000 120,000 180,000
	BlackDiamond 20800 series	120,000
	Summit X450a	5,000
	Summit X480	50,000
	Summit X460, X650, X670	25,000
IS-IS IPv4 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in an L1/L2 IS-IS router.	BlackDiamond 8000 series	20,000
	BlackDiamond 8900 xl-series	20,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	20,000 25,000
	BlackDiamond 12800 series	
	MSM-5, MSM-5R MSM-6R	20,000 25,000
	BlackDiamond 20800 series	20,000
	Summit X450a	3,000
	Summit X460, X480, X650, X670	20,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IS-IS IPv6 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router.	BlackDiamond 8000 series	10,000
	BlackDiamond 8900 xl-series	40,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	30,000 65,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	30,000 40,000 65,000
	BlackDiamond 20800 series	40,000
	Summit X450a	5,000
	Summit X480	25,000
	Summit X460, X650, X670	10,000
IS-IS IPv6 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8000 series	10,000
	BlackDiamond 8900 xl-series	40,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	30,000 65,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	30,000 40,000 65,000
	BlackDiamond 20800 series	40,000
	Summit X450a	5,000
	Summit X480	25,000
	Summit X460, X650, X670	10,000
IS-IS IPv6 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a L1/l2 router.	BlackDiamond 8000 series	10,000
	BlackDiamond 8900 xl-series	15,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	15,000 25,000
	BlackDiamond 12800 series	
	MSM-5, MSM-5R MSM-6R	15,000 25,000
	BlackDiamond 20800 series	15,000
	Summit X450a	3,000
	Summit X480	15,000
	Summit X460, X650, X670	10,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
IS-IS IPv4/IPv6 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8000 series	20,000
	BlackDiamond 8900 xl-series	60,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	60,000 130,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	30,000 60,000 130,000
	BlackDiamond 20800 series	60,000
	Summit X450a	5,000
	Summit X480	40,000
	Summit X460, X650, X670	20,000
IS-IS IPv4/IPv6 L2 routes in an L2 router—recommended maximum number of IS-IS Level 2 routes in a Level 2 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8000 series	20,000
	BlackDiamond 8900 xl-series	60,000
	BlackDiamond 10808	
	MSM-1 MSM-1XL	60,000 130,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	30,000 60,000 130,000
	BlackDiamond 20800 series	60,000
	Summit X450a	5,000
	Summit X480	40,000
	Summit X460, X650, X670	20,000
IS-IS IPv4/IPv6 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a Level 1/Level2 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8000 series	20,000
	BlackDiamond 8900 xl-series	20,000
	BlackDiamond 10808	20,000
	BlackDiamond 12800 series	20,000
	BlackDiamond 20800 series	20,000
	Summit X450a	3,000
	Summit X460, X480, X650, X670	20,000
Jumbo frames—maximum size supported for jumbo frames, including the CRC.	All platforms	9,216
Load-sharing groups—maximum number of load-share groups. **Note:** The actual number of load-share groups that can be configured is limited by the number of physical ports present in the switch or SummitStack.	All platforms (except BlackDiamond 8000 series)	128
	BlackDiamond 8000 series	
	with distributed IP ARP mode off (default) with distributed IP ARP mode on	128 64

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Load sharing—maximum number of ports per load share group.	BlackDiamond 8000 series	8
	BlackDiamond 10808	16
	BlackDiamond 12800 series	16
	BlackDiamond 20800 series	16
	Summit series	8
Logged messages—maximum number of messages logged locally on the system.	All platforms	20,000
MAC-based security—maximum number of MAC-based security policies.	All platforms	1,024
MAC-in-MAC—maximum number of MAC FDB entries (MAC addresses on the local side) and MAC binding entries (MAC addresses on remote side).	BlackDiamond 10808	100,000
	BlackDiamond 12800 series	100,000
MAC-in-MAC—maximum number of regular VLANs (VLAN, VMAN, BVLAN).	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
MAC-in-MAC—maximum number of SVLANs.	BlackDiamond 10808 (1G DRAM)	2,000
	BlackDiamond 12800 series (512 DRAM)	2,000
MAC-in-MAC—maximum number of BVLANs.	BlackDiamond 20800 series	
	per GigE ports	16
	per 10 GigE ports	160
Mirroring (filters)—maximum number of mirroring filters.	BlackDiamond 8000 series	128
	BlackDiamond 10808	64
	BlackDiamond 12800 series	64
	BlackDiamond 20800 series	128
	Summit series	128
Mirroring (monitor port)—maximum number of monitor ports.	All platforms	1
Mirroring, one-to-many (filters)—maximum number of one-to-many mirroring filters.	BlackDiamond 8000 series	128
	BlackDiamond 10808	64
	BlackDiamond 12800 series	64
	BlackDiamond 20800 series	128
	Summit series	128
Mirroring, one-to-many (monitor port)—maximum number of one-to-many monitor ports.	All platforms	16
MLAG ports—maximum number of MLAG ports allowed.	BlackDiamond 8800 series	768
	Summit series	768
MLAG peers—maximum number of MLAG peers allowed.	BlackDiamond 8800 series	1
	Summit series	1

Table 37: Supported Limits (Continued)

Metric	Product	Limit
MPLS LDP enabled interfaces—maximum number of MPLS LDP configured interfaces per switch.	BlackDiamond 8900 xl-series	32
	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
	BlackDiamond 20800 series	50
	Summit X460, X480, X670	32
MPLS LDP peers—maximum number of MPLS LDP peers per switch.	BlackDiamond 8900 xl-series	32
	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
	BlackDiamond 20800 series	64
	Summit X460, X480, X670	32
MPLS LDP adjacencies—maximum number of MPLS LDP adjacencies per switch.	BlackDiamond 8900 xl-series	50
	BlackDiamond 10808	64
	BlackDiamond 12800 series	64
	BlackDiamond 20800 series	64
	Summit X460, X480, X670	50
MPLS LDP ingress LSPs—maximum number of MPLS LSPs that can originate from a switch. * **Note:** The maximum number of ingress LSPs is reduced by one for each transit LSP, that is, If 16,000 transit LSPs are in use, the maximum number of ingress LSPs is 16,000.	BlackDiamond 8900 xl-series	8,000
	BlackDiamond 10808	40,000
	BlackDiamond 12800 R-series	30,000
	BlackDiamond 20800 series	32,000*
	Summit X460 and X480	8,000
	Summit X670	2,048
MPLS LDP transit LSPs—maximum number of MPLS transit LSPs per switch.	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 10808	40,000
	BlackDiamond 12800 R-series	30,000
	BlackDiamond 20800 series	16,000
	Summit X460, X480, X670	4,000
MPLS LDP egress LSPs—maximum number of MPLS egress LSPs that can terminate on a switch.	BlackDiamond 8900 xl-series	8,000
	BlackDiamond 10808	40,000
	BlackDiamond 12800 R-series	30,000
	BlackDiamond 20800 series	32,000
	Summit X460, X480	8,000
	Summit X670	4,096
MPLS static LSPs—maximum number of static LSPs.	BlackDiamond 8900 xl-series	100
	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
	BlackDiamond 20800 series	100
	Summit X460, X480	100
	Summit X670	10

Table 37: Supported Limits (Continued)

Metric	Product	Limit
MSDP active peers—maximum number of active MSDP peers.	BlackDiamond 8000 series	32
	BlackDiamond 8900 series	64
	BlackDiamond 10808	32
	BlackDiamond 12800 series	32
	BlackDiamond 20800 series	64
	Summit X460, X480, X650, X670	16
MSDP SA cache entries—maximum number of entries in SA cache.	BlackDiamond 8000 series	16,000
	BlackDiamond 8900 series	16,000
	BlackDiamond 10808	16,000
	BlackDiamond 12800 series	16,000
	BlackDiamond 20800 series	15,000
	Summit X460, X480, X650, X670	8,000
MSDP maximum mesh groups—maximum number of MSDP mesh groups.	BlackDiamond 8000 series	8
	BlackDiamond 8900 series	16
	BlackDiamond 10808	8
	BlackDiamond 12800 series	8
	BlackDiamond 20800 series	16
	Summit X460, X480, X650, X670	4
Multicast VLAN registration (MVR)—maximum number of MVR senders per switch (IP multicast compression disabled).	BlackDiamond 8800 a-series	1,024
	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 series	
	8900-10G24X-c modules 8900-G96T-c modules 8900 xl-series 8900-40G6X-xm	2,048[c] 4,096[c] 4,096[c] 3,000[d]
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	BlackDiamond 20800 series	3,700
	Summit X150, X250, X350, X450e	500[d]
	Summit X450a	1,024
	Summit X480	4,096
	Summit X460	2,048
	Summit X650	2,048
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Multicast VLAN registration (MVR)—maximum number of MVR senders per switch (IP multicast compression enabled).	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 c-series	6,000[d]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 c-series	6,000[d]
	BlackDiamond 8900 xl-series	12,000[b]
	8900-40G6X-xm module	3,000[d]
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	2,000[d]
	Summit X460	6,000[d]
	Summit X480	12,000[b]
	Summit X650	6,000[d]
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]
Network login—maximum number of clients being authenticated on MAC-based VLAN enabled ports.	BlackDiamond 8000 series (clients per module/per system)	1,024
	BlackDiamond 12804 (per system)	4,000
	Summit series	1,024
Network login—maximum number of dynamic VLANs.	All platforms (except the BlackDiamond 20800 series)	2,000
Network login VLAN VSAs—maximum number of VLANs a client can be authenticated on at any given time.	All platforms	10
OSPF adjacencies—maximum number of supported OSPF adjacencies.	BlackDiamond 8000 series	128
	BlackDiamond 8900 xl-series	255
	BlackDiamond 10808	255
	BlackDiamond 12800 series	255
	BlackDiamond 20800 series	255
	Summit X250e, X460, X650, X670	128
	Summit X480	255
OSPF areas—as an ABR, how many OSPF areas are supported within the same switch.	All platforms	8
OSPF ECMP—maximum number of equal cost multipath OSPF.	BlackDiamond 8000 series	2, 4, or 8
	BlackDiamond 10808	8
	BlackDiamond 12800 series	8
	BlackDiamond 20800 series	8
	All Summit series	2, 4, or 8

Table 37: Supported Limits (Continued)

Metric	Product	Limit
OSPF external routes—recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	BlackDiamond 8000 series	20,000
	BlackDiamond 8900 xl-series	130,000
	BlackDiamond 10808	130,000
	BlackDiamond 12800 series	130,000
	BlackDiamond 20800 series	130,000
	Summit X250e, X450a, X460, X650, X670	5,000
	Summit X480	130,000
OSPF inter- or intra-area routes—recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	BlackDiamond 8000 series	7,000
	BlackDiamond 8900 xl-series	7,000
	BlackDiamond 10808	7,000
	BlackDiamond 12800 series	7,000
	BlackDiamond 20800 series	7,000
	Summit X250e, X450a, X460, X650, X670	2,000
	Summit X480	7,000
OSPF routers in a single area—recommended maximum number of routers in a single OSPF area.	BlackDiamond 8000 series	100
	BlackDiamond 8900 xl-series	200
	BlackDiamond 10808	200
	BlackDiamond 12800 series	100
	BlackDiamond 20800 series	200
	Summit X250e, X450a, X460, X650, X670	50
	Summit X480	200
OSPF subnets on a single router—recommended maximum number of OSPF routed subnets on a switch.	All platforms with Core license or higher	400
OSPF virtual links—maximum number of supported OSPF virtual links.	All platforms with Core license or higher	32
OSPFv2 links—maximum number of links in the router LSA.	All platforms	419
OSPFv3 active interfaces—maximum number of OSPFv3 active interfaces.	All platforms with Advanced Edge license	4
OSPFv3 areas—as an ABR, the maximum number of supported OSPFv3 areas.	All platforms with Core license or higher	16
OSPFv3 external routes—recommended maximum number of external routes.	BlackDiamond 8000 series	10,000
	BlackDiamond 8900 xl-series	60,000
	BlackDiamond 10808	60,000
	BlackDiamond 12800 series	50,000
	BlackDiamond 20800 series	60,000
	Summit X450a, X460, X650, X670	10,000
	Summit X480	60,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
OSPFv3 interfaces—maximum number of OSPFv3 interfaces.	BlackDiamond 8000 series	256
	BlackDiamond 8900 xl-series	384
	BlackDiamond 10808	384
	BlackDiamond 12800 series	256
	BlackDiamond 20800 series	384
	Summit X450a, X460, X650, X670	128
	Summit X480	384
OSPFv3 inter- or intra-area routes—recommended maximum number of inter- or intra-area routes.	BlackDiamond 8000 series	6,000
	BlackDiamond 8900 xl-series	6,000
	BlackDiamond 10808	6,000
	BlackDiamond 12800 series	6,000
	BlackDiamond 20800 series	6,000
	Summit X450a, X460, X650, X670	3,000
	Summit X480	6,000
OSPFv3 neighbors—maximum number of OSPFv3 neighbors.	BlackDiamond 8000 series	64
	BlackDiamond 8900 xl-series	128
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	BlackDiamond 20800 series	128
	Summit X450a, X460, X650, X670	64
	Summit X480	128
OSPFv3 virtual links—maximum number of OSPFv3 virtual links supported.	All platforms with Core license or higher	16
PIM snooping—maximum number of (S,G) entries programmed in the hardware (IP multicast compression disabled).	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 8000 e-series	500[c]
	BlackDiamond 8900 series	
	8900-10G24X-c modules	2,048[c]
	8900-G96T-c modules	4,096[c]
	8900 xl-series	4,096[c]
	8900-40G6X-xm	3,000[d]
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	BlackDiamond 20800 series	3,700
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	1,024
	Summit X480	4,096
	Summit X460	2,048
	Summit X650	2,048
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
PIM snooping—maximum number of (S,G) entries programmed in the hardware (IP multicast compression enabled).	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 c-series	6,000[d]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 c-series	6,000[d]
	BlackDiamond 8900 xl-series	12,000[b]
	8900-40G6X-xm	3,000[d]
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	2,000[d]
	Summit X480	12,000[b]
	Summit X460	6,000[d]
	Summit X650	6,000[d]
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]
PIM—maximum routes—maximum number of (S,G) entries installed in the hardware (IP multicast compression disabled).	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 series	
	8900-10G24X-c modules 8900-G96T-c modules 8900 xl-series 8900-40G6X-xm	2,048[c] 4,096[c] 4.096[c] 3,000[d]
	BlackDiamond 10808	12,000
	BlackDiamond 12800 series	12,000
	BlackDiamond 20800 series	3,700
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	1,024
	Summit X480	4,096
	Summit X460	2,048
	Summit X650	2,048
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
PIM—maximum routes—maximum number of (S,G) entries installed in the hardware (IP multicast compression enabled).	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 c-series	6,000[d]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 c-series	6,000[d]
	BlackDiamond 8900 xl-series	12,000[b]
	8900-40G6X-xm modules	3,000[d]
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	1,024
	Summit X480	12,000[b]
	Summit X460	2,048
	Summit X650	2,048
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]
PIM-SSM (maximum SSM routes)—maximum number of (S,G) entries installed in the hardware with PIM SSM configuration (IP multicast compression disabled).	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 series	
	8900-10G24X-c modules 8900-G96T-c modules 8900 xl-series 8900-40G6X-xm	2,048[c] 4,096[c] 15,000 3,000[d]
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	4,096[c]
	BlackDiamond 20800 series	3,700
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	1,024
	Summit X480	4,096
	Summit X460	2,048
	Summit X650	2,048
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]

Table 37: Supported Limits (Continued)

Metric	Product	Limit
PIM-SSM (maximum SSM routes)—maximum number of (S,G) entries installed in the hardware with PIM SSM configuration (IP multicast compression enabled).	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 c-series	6,000[d]
	BlackDiamond 8000 e-series	500[d]
	BlackDiamond 8900 c-series	6,000[d]
	BlackDiamond 8900 xl-series	12,000[b]
	8900-40G6X-xm	3,000[d]
	Summit X150, X250e, X350, X450e	500[d]
	Summit X450a	2,000[d]
	Summit X480	12,000[b]
	Summit X460	6,000[d]
	Summit X650	6,000[d]
	VIM3-40G4x	3,000[d]
	Summit X670	
	VIM4-40G4x	3,000[d]
PIM (maximum interfaces)—maximum number of PIM active interfaces.	All platforms	256
PIM (maximum interfaces)—maximum number of PIM snooping enabled interfaces.	All platforms	256
Policy-based routing (PBR) redundancy—maximum number of flow-redirect and nexthops per each flow-direct.	All platforms	32
Private VLANs—maximum number of subscribers. Assumes a minimum of one port per network and subscriber VLAN.	BlackDiamond 8800 a-, c-, e-, xl-series	
	with eight modules of 48 ports 8900-G96T-c modules	383 767
	BlackDiamond 10808	1,400
	BlackDiamond 12800 series	1,400
	Summit series	One less than the number of available user ports
Private VLANs—maximum number of private VLANs with an IP address on the network VLAN. **Note:** This limit is dependent on the maximum number of private VLANs in an L2-only environment if the configuration has tagged and translated ports.	All platforms	512
Private VLANs—maximum number of private VLANs in an L2-only environment.	BlackDiamond 8800 a-, c-, e-series	384
	BlackDiamond 8900 series	2,046
	BlackDiamond 10808	2,046
	BlackDiamond 12800 series	2,046
	Summit X250e, X450a, X450e, X460	384
	Summit X480, X650, X670	2,046
Provider Backbone Bridging (PBB) Service and Customer VLANs—maximum number of service and customer VLANs	BlackDiamond 20800 series	4,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
PBB Backbone VLANs—maximum number of backbone VLANs.	BlackDiamond 20800 series	2,000
PBB ISIDs—maximum number of ISIDs. Range is 256 to 330, 221.	BlackDiamond 20800 series	4,000
PBB Backbone Edge Bridges (BEBs) in a PBB Network—maximum number of BEBs in a PBB network.	BlackDiamond 20800 series	256
PBB MAC Binding Entries—maximum number of MAC-binding entries.	BlackDiamond 20800 series	400,000
PBB-Traffic Engineering (PBB-TE)—maximum number of static MAC binding entries.	BlackDiamond 10808 MSM-1 MSM-1XL BlackDiamond 12800 series MSM-5 MSM-5R MSM-6R	 98,000 100,000 49,000 100,000 100,000
Route policies—suggested maximum number of lines in a route policy file.	All platforms	10,000
RIP-learned routes—maximum number of RIP routes supported without aggregation.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond 10808 BlackDiamond 20800 series Summit X250e, X450a Summit X460 Summit X480, X650, X670	10,000 10,000 10,000 10,000 3,000 10,000 10,000
RIP interfaces on a single router—recommended maximum number of RIP routed interfaces on a switch.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond 10808 BlackDiamond 20800 series Summit X250e, X450a Summit X460 Summit X480 Summit X650, X670	256 384 384 384 128 256 384 256
RIPng learned routes—maximum number of RIPng routes.	BlackDiamond 8000 series BlackDiamond 8900 xl-series BlackDiamond 10808 BlackDiamond 12800 series BlackDiamond 20800 series Summit X250e, X450a Summit X480 Summit X460, X650, X670	3,000 5,000 5,000 5,000 5,000 1,500 5,000 3,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
RSVP-TE interfaces—maximum number of interfaces.	BlackDiamond 8900 xl-series	32
	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
	BlackDiamond 20800 series	64
	Summit X460, X480, X670	32
RSVP-TE ingress LSPs—maximum number of ingress LSPs.	BlackDiamond 8900 xl-series	2,000
	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	2,000
	BlackDiamond 20800 series	2,000
	Summit X460, X480, X670	2,000
RSVP-TE egress LSPs—maximum number of egress LSPs.	BlackDiamond 8900 xl-series	2,000
	BlackDiamond 10808	4,000
	BlackDiamond 12800 R-series	4,000
	BlackDiamond 20800 series	4,000
	Summit X460, X480, X670	2,000
RSVP-TE neighbors—maximum number of neighbors per interface.	Summit X670	64
RSVP-TE transit LSPs—maximum number of transit LSPs.	BlackDiamond 8900 xl-series	2,000
	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	1,500
	BlackDiamond 20800 series	2,000
	Summit X460, X480, X670	2,000
RSVP-TE paths—maximum number of paths.	BlackDiamond 8900 xl-series	1,000
	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
	BlackDiamond 20800 series	1,000
	Summit X460, X480	1,000
RSVP-TE profiles—maximum number of profiles.	BlackDiamond 8900 xl-series	1,000
	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
	BlackDiamond 20800 series	1,000
	Summit X460, X480	1,000
RSVP-TE EROs—maximum number of EROs per path.	BlackDiamond 8900 xl-series	64
	BlackDiamond 10808	64
	BlackDiamond 12800 R-series	64
	BlackDiamond 20800 series	64
	Summit X460, X480	64
Spanning Tree (maximum STPDs)—maximum number of Spanning Tree Domains on port mode EMISTP.	All platforms	64

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Spanning Tree PVST—maximum number of port mode PVST domains. **Notes:** • Maximum of 7 active ports per PVST domain when 128 PVST domains are configured. • For the Black Diamond 20800 series switch, there is a maximum of 10 active ports per PVST domain when 256 PVST domains are configured,	All platforms (except BlackDiamond 20800 series) BlackDiamond 20800 series	128 256
Spanning Tree—maximum number of multiple spanning tree instances (MSTI) domains.	All platforms	64
Spanning Tree—maximum number of VLANs per MSTI. **Note:** Maximum number of 10 active ports per VLAN when all 500 VLANs are in one MSTI.	All platforms (except Summit X460) Summit X460	500 600
Spanning Tree—maximum number of VLANs on all MSTP instances.	All platforms (except BlackDiamond 20800 series and Summit X460) BlackDiamond 20800 series Summit X460	1,000 1,024 1,024
Spanning Tree (802.1d domains)—maximum number of 802.1d domains per port.	All platforms	1
Spanning Tree (number of ports)—maximum number of ports including all Spanning Tree domains.	All platforms	2,048
Spanning Tree (maximum VLANs)—maximum number of STP protected VLANs (dot1d and dot1w).	BlackDiamond 8900 series BlackDiamond 20800 series Summit X460 All other platforms	1,024 1,024 600 560
SSH (number of sessions)—maximum number of simultaneous SSH sessions.	All platforms	8
Static MAC multicast FDB entries—maximum number of permanent multicast MAC entries configured into the FDB.	BlackDiamond 8000 a-, c-, e-, xl-series BlackDiamond 10808 BlackDiamond 12800 series Summit X150, X350, X250e, X450a, X450e, X460, X480, X650, X670	1,024 1,024 1,024 1,024
Syslog servers—maximum number of simultaneous syslog servers that are supported.	All platforms	4
TCAM entries—amount of entries available in the lookup tables for Longest Prefix Match routing lookups, learned MAC address, and ACLs.	BlackDiamond 10808, MSM-1 BlackDiamond 10808, MSM-1XL BlackDiamond 12800 series BlackDiamond 12800 R-series BlackDiamond 20800 series	128,000 256,000 49,000 229,000 128,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
Telnet (number of sessions)—maximum number of simultaneous Telnet sessions.	All platforms	8
Virtual routers—maximum number of user-created virtual routers that can be created on a switch. **Note:** Virtual routers are not supported on Summit X150, X250e, X350, X450a, and X450e series switches.	BlackDiamond 8000 c-, xl-, xm-series BlackDiamond 10808 BlackDiamond 12800 series BlackDiamond 20800 series Summit X460, X480, X650, X670	63 63 63 63 63
Virtual router forwarding (VRFs)—maximum number of VRFs that can be created on a switch. **Note:** VPN VRFs are not supported in ExtremeXOS 12.6.2.	BlackDiamond 8000 c-, xl-, xm-series BlackDiamond 10808 BlackDiamond 12800 series BlackDiamond 20800 series Summit X460, X480, X650, X670	190 1000 1000 1000 190
VRF forwarding instances—number of non-VPN VRFs that can be created on a switch.	BlackDiamond 8000 c-, xl-, xm-series BlackDiamond 10808 BlackDiamond 12800 series BlackDiamond 20800 series Summit X460, X480, X650, X670	190 800 800 400 190
Virtual router protocols per VR—maximum number of routing protocols per VR.	All platforms	8
Virtual router protocols per switch—maximum number of VR protocols per switch.	All platforms	64
VLAN aggregation—maximum number of port-VLAN combinations on any one super VLAN and all of its sub VLANs.	All platforms	1,000
VLANs—includes all VLANs.	All platforms	4,094
VLANs—maximum number of virtual ports.	BlackDiamond 12804 BlackDiamond 20800 series	50,029 50,029
VLANs (Layer 2)—maximum number of Layer 2 VLANs.	All platforms	4,094
VLANs (Layer 3)—maximum number of Layer 3 VLANs.	All platforms	512
VLANs (maximum active port-based)—number of simultaneously active port-based VLANs.	All platforms	4,094
VLANs (maximum active protocol-sensitive filters)—number of simultaneously active protocol filters in the switch.	All platforms	15

Table 37: Supported Limits (Continued)

Metric	Product	Limit
VLAN translation—maximum number of translation VLANs. Assumes a minimum of one port per translation and member VLAN.	BlackDiamond 8000 a-, c-, e-, xl-series	
	with eight modules of 48 ports 8900-G96T-c modules	383 767
	BlackDiamond 10808	1,400
	BlackDiamond 12800 series	1,400
	Summit X450a and X450e, group of 24 ports	
	with two-port option cards without option cards	25 23
	Summit series	One less than the number of available user ports
VLAN translation—maximum number of translation VLAN pairs with an IP address on the translation VLAN. **Note:** This limit is dependent on the maximum number of translation VLAN pairs in an L2-only environment if the configuration has tagged and translated ports.	All platforms	512
VLAN translation—maximum number of translation VLAN pairs in an L2-only environment.	BlackDiamond 8800 a-, c-, e-series	384
	BlackDiamond 8900 xl-series	2,046
	BlackDiamond 10808	2,046
	BlackDiamond 12800 series	2,046
	Summit X250e, X450a, X450e, X460	384
	Summit X480, X650, X670	2,046
VMAN (maximum ACL rules for VMAN)—maximum number of ACL rules for VMAN.	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
VMAN (0x8100 ethertype VMANs)—maximum number of VMANs configured on a port whose ethertype is 0x8100.	BlackDiamond 20800 series	4,092
VPLS: VCCV (pseudo wire Virtual Circuit Connectivity Verification) VPNs—maximum number of VCCV enabled VPLS VPNs.	BlackDiamond 8900 xl-series	16
	BlackDiamond 10808	16
	BlackDiamond 12800 R-series	16
	BlackDiamond 20800 series	16
	Summit X460, X480, X670	16
VPLS: MAC addresses in an H-VPLS network—maximum number of MAC address learned by a switch in an evenly distributed hierarchical VPLS **Note:** Increasing the number of spokes per VPLS will decrease the maximum number of MAC addresses that can be learned.	BlackDiamond 10808	60,000
	BlackDiamond 12800 R-series	60,000
VPLS: MAC addresses in a fully meshed VPLS network—maximum number of MAC addresses learned by a switch in an evenly distributed fully meshed VPLS network.	BlackDiamond 10808	100,000
	BlackDiamond 12800 R-series	80,000

Table 37: Supported Limits (Continued)

Metric	Product	Limit
VPLS: MAC addresses—maximum number of MAC addresses learned by a switch.	BlackDiamond 8900 xl-series	524,288 (up to)[b]
	BlackDiamond 20800 series	500,000
	Summit X460	32,768
	Summit X480	524,288 (up to)[b]
	Summit X670	128,000
VPLS VPNs—maximum number of VPLS virtual private networks per switch.	BlackDiamond 8900 xl-series	1,023
	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	2,000
	BlackDiamond 20800 series	4,000
	Summit X460, X480, X670	1,023
VPLS peers—maximum number of VPLS peers per VPLS instance.	BlackDiamond 8900 xl-series	32
	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
	BlackDiamond 20800 series	64
	Summit X460, X480, X670	32
VPLS pseudo wires—maximum number of VPLS pseudo wires per switch.	BlackDiamond 8900 xl-series	7,090
	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	2,000
	BlackDiamond 20800 series	16,000
	Summit X460, X480	7,090
	Summit X670	4,000
Virtual Private Wire Service (VPWS) VPNs—maximum number of virtual private networks per switch.	BlackDiamond 8900 xl-series	4,000
	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
	BlackDiamond 20800 series	4,000
	Summit X460	1,000
	Summit X480	4,000
	Summit X670	2,047
VRRP (maximum instances)—maximum number of VRRP instances for a single switch.	BlackDiamond 8800 c-series	
	MSM-48c	256
	BlackDiamond 8900 xl-series	
	8900-MSM128	256
	BlackDiamond 20800 series	256
	All other platforms with Advanced Edge license or higher	128
VRRP (maximum VRID)—maximum number of unique VRID numbers per switch.	All platforms with Advanced Edge license or higher	7
VRRP (maximum VRIDs per VLAN)—maximum number of VRIDs per VLAN.	All platforms with Advanced Edge license or higher	7
VRRP (maximum ping tracks)—maximum number of ping tracks per VLAN.	All platforms with Advanced Edge license or higher	8

Table 37: Supported Limits (Continued)

Metric	Product	Limit
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances. **Hello interval:** 100 milliseconds Frequency: 3 seconds Miss: 3 **Hello interval:** 1 second Frequency: 3 seconds Miss: 3	All platforms with Advanced Edge license or higher	 2 4
VRRP (maximum iproute tracks)—maximum number of IP route tracks per VLAN.	All platforms with Advanced Edge license or higher	8
VRRP—maximum number of VLAN tracks per VLAN.	All platforms with Advanced Edge license or higher	8
XML requests—maximum number of XML requests per second. **Note**: Limits are dependent on load and type of XML request. These values are dynamic ACL data requests.	BlackDiamond 8800 c-series with 100 DACLs with 500 DACLs BlackDiamond 8900 series with 100 DACLs with 500 DACLs BlackDiamond 12800 series with MSM-6R with 100 DACLs with 500 DACLs Summit X450a, X480, X650, X670 with 100 DACLs with 500 DACLs	 10 3 10 3 10 3 4 1
XNV authentication—maximum number of VMs that can be processed (combination of local and network VMs).	All platforms	2,048
XNV database entries—maximum number of VM database entries (combination of local and network VMs).	All platforms	16,000
XNV database entries—maximum number of VPP database entries (combination of local and network VPPs).	All platforms	2,048
XNV local VPPs—maximum number of XNV local VPPs.[e]	All platforms Ingress Egress	 2,048 512
XNV network VPPs—maximum number of XNV network VPPs.[e]	All platforms Ingress Egress	 2,048 512

a. The table shows the total available; see the note included in PD3-77983510.
b. Limit depends on setting configured for `configure forwarding external-tables`.
c. Applies only if all enabled BlackDiamond 8000 I/O modules are BlackDiamond 8000 c-, xl-, or xm-series modules.
d. Effective capacity varies based on actual IP addresses and hash algorithm selected, but is higher for BlackDiamond 8000 c-, xl-, xm-series modules and Summit X460, X480, X650, and X670 switches compared to BlackDiamond 8800 a-series and 8000 e-series modules and Summit X250e, X450e, and X450a switches.
e. The number of XNV authentications supported based on system ACL limitations.

3 CHAPTER Open Issues, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification and behaviors that might not be intuitive. It also includes the items that have been resolved.

This chapter contains the following sections:

- Open Issues on page 67
- Known Behaviors on page 81
- Resolved Issues in ExtremeXOS 12.6.2-patch1-9 on page 84
- Resolved Issues in ExtremeXOS 12.6.2-patch1-8 on page 84
- Resolved Issues in ExtremeXOS 12.6.2-patch1-5 on page 86
- Resolved Issues in ExtremeXOS 12.6.2-patch1-3 on page 88
- Resolved Issues in ExtremeXOS 12.6.2-patch1-2 on page 90
- Resolved Issues in ExtremeXOS 12.6.2 on page 92
- Resolved Issues in ExtremeXOS 12.6.1 on page 95

Open Issues

Following are the open issues for supported features in ExtremeXOS 12.6.2.

Table 38: Open Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2110742669	When using SCP to transfer files to an Extreme switch, the transfer fails with an "incomplete command" error.
PD4-1885807081	A switch shows the following ACL error while detecting a kerberos identity and the switch is not synchronizing the kerberos identity with a backup slot. `<Erro:HAL.IPv4ACL.Error>`
PD4-1688055111	A system crash occurs when the system is configured with 2,000 VPLS and 1,000 CFM instances while running the restart ports, or save and reboot commands.
PD4-1663984367	Whenever a (*, G) join is received, all hardware entries installed on non upstream (*, G) interfaces are cleared. Therefore, every 60 seconds, the L2 switching is affected, traffic comes to the CPU, and entries are re-learned.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1630086252	When unconfiguring an IP address on an egress VLAN, or re-configuring the IP address of the egress VLAN, all the MVR cache entries that are ingressing via other VLANs are also cleared from the hardware. Because of this, momentary CPU bursts are observed.
PD4-1820554590	A switch sends an MLDv2 listener report even though MLDv1 is enabled on the switch.
PD4-1820554531	While running a TAHI conformance suite for MLDv2, a switch always sets the QQI value to 0 in MLDv2 general query messages. It should set QQI to querier query interval.
PD4-1842342875, PD4-1466022175	When an SNMP query is issued for non-existent IPv4 routes, the RtMgr process crashes with signal 11.
PD4-1842342767, PD4-1300978095	After installing a legacy CLI module, the CLI command `load script` returns the following error message: `%% Unrecognized command: create vlan v$x`
PD4-1771325794, PD4-770508534	If the `configure ip-mtu` command is configured on VLANs that have only an IPv6 address, the `show configuration` command does not display the output for the `configure ip-mtu` command.
PD4-1540274936	An ISIS process crash with signal 6 may occur when disabling ISIS when ISISv6 and ISIS IP route compression are configured.
PD4-1584840651	The ethernet OAM half-link feature is not supported in ExtremeXOS 12.6.1.
PD4-1556309411	With multiple NSSA areas where there is more than one link between areas, OSPF default routes are not installed in the routing table.
PD4-1549189647	In ISIS, when route summarization is configured with authentication, the authentication is not effective and all the routes are advertised, regardless of the type of authentication configured.
PD4-1535268629	ISIS tx-only authentication also authenticates received LSPs. The received routes are not installed in the ISIS LSDB based on the authentication policy.
PD4-1620486143	When DHCP lease time is set to the maximum/infinity (4294967295), the DHCP client continuously sends renewal requests.
PD3-57182431	For the incoming traffic with alignment errors, the "RX Align" counter in the output of the `show ports <port number> rxerrors` command is not incremented. Instead, the "RX CRC" counter is incremented.
PD4-813961562	When a service VLAN is changed to include a dot1q tag on both sides in CFM VPLS, the RMEP entry is not learned on one side.
PD4-749060484	Errors are seen when a configuration having identifiers (SNMPv3 user name/EAPS domain name) with special characters are loaded through a script.
PD4-561358261	If you create a super VLAN and a sub-VLAN in different virtual routers you are able to bind the VLANs. Super VLANs and sub-VLANs should belong to the same virtual router.
PD4-460892051	Installing different versions of an ExtremeXOS image and an SSH image displays the following error message: `Failed to install image- cannot read spec file" in the log "upgrade failed installation:got error from installer DLL"`
PD3-132508261	When issuing the `enable jumbo-frame port all` command on a BlackDiamond 8800, the MTU size for the VLAN is not configured. Sending 5,000 byte traffic works correctly. However, if you disable jumbo-frames on the egress port the error message `Packet too big` is displayed.
PD3-104885349	When a shared link comes up, temporary traffic loss may occur until FDB entries are aged. Aging occurs by default every five minutes. **Workaround:** To reduce traffic loss, reduce the default age time.
PD3-132775269	Telnet sessions between two switches using two windows causes one session to hang if both sessions are edited but only one session is saved.
PD3-28378521	Enabling load sharing on a port that is being mirrored causes the mirroring to stop.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
BlackDiamond 8800 Series Switches	
PD4-2166404788	Some software forwarding of untagged VMAN traffic does not work when an 8900-MSM128 module is installed.; That is, the software forwarding that results when limit-learning is configured does not work. A similar problem occurs with untagged VMAN traffic received from one of the following I/O modules regardless of the MSM installed: • 8900-G48T-xl • 8900-G48X-xl • 8900-G96Tc • 8900-10G8X-xl • 10G8Xc • 10G4Xc This problem is also seen in ExtremeXOS 12.3, 12.4, and 12.5 software releases.
PD4-2049460356	Only partial traffic is forwarded between a service VLAN and VPLS (LACP). Transmitting from a VLAN to VPLS, traffic loss is approximately 10%; from VPLS to a VLAN, traffic loss is approximately 98%.
PD4-1633677741	On a BlackDiamond 8800 series switch, making link state changes during a large policy refresh can take more than 20 seconds and may cause duplicate packet forwarding in an MLAG configuration.
PD4-1680990961	Process etmon is terminated with signal 6 on MSM-B during local AAA feature regression.
PD4-1546542587	ISIS process crashes with signal 6 while trying to change the metric-style to `wide` under scaled conditions.
PD4-1637972971	Beginning with ExtremeXOS 12.5, the mirroring feature stops working after downgrading and then upgrading the switch software.
PD4-1659977270	A BlackDiamond 8810 switch does not forward L3 routed packets with MPLS PHP enabled. **Workaround:** Disable MPLS PHP.
PD4-1567438997	When an ExtremeXOS switch receives an OSPF user group LSA advertisement with a router ID field as 0.0.0.0, the switch does not process the advertisement and reboots OSPF.
PD4-1674379381	When installing new PSU controller firmware, log messages starting with `<Crit:Kern.Critical>` or `<Erro:Kern.Error>` may be generated by the backup MSM and can be ignored.
PD4-1627772844	Due to the addition of new features in ExtremeXOS 12.5, BlackDiamond 8800 series switch configurations running older management modules (MSM-G8X and MSM-48) may run out of memory when a large number of VLANs are configured with multiple tagged ports added for each VLAN. For example, a configuration with 4,000 VLANs and 24 ports tagged on each VLAN is not supported. Newer BlackDiamond 8800 management modules (MSM-48c or 8900-MSM128) are recommended for larger configurations.
PD4-1530729359	An OSPF session goes down and stays in EX_START and continues flapping to EXCHANGE and EX_START states.
PD4-750014887	If a failover occurs during a “refresh policy” the HAL process dies on a new master MSM. **Workaround:** Avoid performing a policy refresh if switching from one MSM to another.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
BlackDiamond 10800 Series Switches	
PD4-718946965	Directed broadcast traffic is not forwarded if MPLS PHP is enabled.
PD4-1621694181	The following error is seen on a BlackDiamond 10800 series switch when it reboots with a DHCP client configuration. `<Erro:cm.sys.actionErr> MSM-A: Error while loading "ipBrForward":` **Workaround:** Run the show log match error command again.
PD4-1603284873	Route compression is not working properly when a system experiences a TCAM full condition.
PD3-121985381	You cannot configure an IP MTU that is greater than the configured jumbo frame size. However, when the jumbo frame size is configured using a smaller value than the IP MTU, the configuration is accepted and the traffic is forwarded using the larger packet sizes.
PD4-489592307	Switch is not sending an "icmp destination unreachable" message to the source when it receives a jumbo packet with a "don't fragment" bit message. This applies to BlackDiamond 10800 and BlackDiamond 20808 switches only.
PD3-28320363	In IPv6, the encapsulate value is "next header," which is not currently a valid attribute.

PD3-124124316	The following error messages are shown in the log when running 50,000 unicast routes with ECMP enabled:
	`<Warn:HAL.Sys.Warning> MSM-A: hal: Reached maximum otp index allocation`
	`<Warn:HAL.Sys.Warning> MSM-A: Previous message repeated 999 additional times in the last 1 second(s)`

PD4-318846862	L3 multicast traffic in a VPLS VMAN is forwarded twice when the LSP is changed to port sharing and is then changed back.
PD3-54870537, PD3-45729158	Under the following circumstances, EAPS control packets received on the wrong VLAN may be treated and processed. **1** Create a EAPS ring with three or more switches with a BlackDiamond 10808 as one of the transit switches, directly connect to the master with load sharing enabled. **2** Enable load sharing on the primary port of the master switch (the master port should be higher than the group port so that the configuration master and current master are different in load sharing). **3** Disable load sharing on the BlackDiamond 10808. **4** Show EAPS on the master switch; the domain state will be complete. **5** The control packets are transmitted on the current master and the BlackDiamond 10808 will receive the packets on the port that is not part of the EAPS VLAN.
PD3-202184409	Adding/deleting a LAG sharing port changes the VLAN status, which is causing an OSPF/MPLS reconvergence.
PD3-133427241	When an OSPF external filter is configured to deny routes, not all routes are being filtered.
PD3-204793983	The egress rate-limit shown in the command output of the `show port utilization` command is not correct.
BlackDiamond 12800 Series Switches	
PD4-1598681891	When a BlackDiamond 12800 series switch is transmitting EAPS traffic, a dual master situation occurs and the backup MSM goes into a failed state causing the system to reboot with a higher number of routes and traffic.
PD4-1576028451	Error messages are displayed on the console when an MSM failover is performed, and when a PBB configuration exists with a high number of service VLANs.
PD4-722565430	IPv6 ACL address masks are not working correctly after rebooting a switch.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-737811617	Creating a blackhole FDB entry on a BlackDiamond 12800 series switch still forwards traffic from a BlackDiamond 20808 to a BlackDiamond 12800. **Workaround:** Create blackhole entries for the same MAC on each of the subscriber VLANs.
PD4-742951283	An I/O slot fails due to a Tx data memory overflow and generates the following error message: `<Erro:HAL.Card.Error> MSM-A: skylerHC-1184: skyler12 on slot 1 (4 errors):TX Data Memory Overflow: reg 0x32 value 0x01000001 wanted (0x00000000) got (0x01000000)`
PD4-740255437	Policy files are not refreshed when generating 30,000 rules.
PD4-285686375	After upgrading to the latest ExtremeXOS 12.1.2. image, the following EEPROM error message appears in the log: `MSM-A: MSM-B card eeprom checksum failed. 0xb97 != 0xb96`
PD3-125288233	MSTP fails to converge when a VMAN Ethernet type is set to 0x8100 on a BlackDiamond 12800 series switch.
PD3-192175421	The following error message is displayed when installing a policy file with more than 4,096 rules: `Error: Unable to bind traffic queue tq4095 to port 1:1.`
PD3-187808062	A BlackDiamond 12800 series switch does not show a warning message on the console for down revision MSM and I/O modules after initialization.
PD3-86738591	Traffic queue statistics are incorrect when a BlackDiamond 12800 series switch is configured to work in H-QoS mode. Statistics counters are accurate when the switch is configured in the PRI mode.
PD3-118914021	When an OSPF neighbor is configured between two LSRs and MPLS, and an LDP session is configured between them, the ABR router advertises a default route to the internal router. The default route is not mapped to a label in the internal router because the ABR does not advertise the label
BlackDiamond 20800 Series Switches	
PD4-2053199356	OSPFv3 neighbors move to INIT after executing the run msm-failover command.
PD4-1630086359	A BlackDiamond 20800 series switches displays critical error messages and becomes unstable when multicast traffic is received when there are 200 egress interfaces.
PD4-1545944959	With 255 adjacencies, some of the adjacent OSPF peers are in different states, for example, one side shows OSPF neighbors are full, and the other side shows they are still in the exchange state.
PD4-1595073183	After flapping an aggregate-address, you cannot create or delete a BGP aggregate-address.
PD4-1851065971	During a reboot or when running the `unconfigure switch` command, the following warning message may be displayed: `CPU 0: soft watchdog expiration warning & CPU 0: Kernel thread was stuck`
PD4-1689076501	Rebooting a BlackDiamond 20800 series switch causes the system to crash in process HAL signal 11.
PD4-1369879610	Disabling a slot on a BlackDiamond 20800 series switch while booting the system removes the module type.
PD4-1593913298	When multiple VPLS instances are configured on a BlackDiamond 20800 series switch to one peer, and the VPLS instances use different RSVP-TE LSPs for pseudo wire transport, traffic for some VPLS instances may be dropped.
PD4-1633907245	A primary MSM fails and reboots because of a dual master MSM while downloading and installing a new image using a larger number of routes and traffic.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1564628282	High CPU utilization is seen when broadcast traffic is sent over a VPLS service VLAN or VMAN.
PD4-1586685991	Traffic is not shaped on a BlackDiamond 20800 series switch if ports are added to a VMAN after configuring an ACL.
PD4-1394425195	DUT allows you to create large traffic queues without displaying an error message. The system may reboot, or I/O modules could reboot and go into a failed state, when creating and binding traffic queues that exceed the limit.
PD4-1614019101	After running the restart process vrrp command on a BlackDiamond 20800 series switch VRRP master, the switch may initiate slowpath forwarding. **Workaround:** Run the `restart process vrrp` command again.
PD4-1594401361	ESRP flapping causes errors on a BlackDiamond 20800 series switch that is configured with 128 ESRP domains and 2,944 VLANs.
PD4-730221901	Refreshing an ACL on an MM-B while running an MSM failover on MM-A causes MSM-A to lose the ACL configuration on MSM-A.
PD4-646084932	An FDB entry for a non-isolated VLAN is not show in the output of the `show fdb` command after disabling and enabling an I/O module.
PD4-733230780	MAC security does not work on a PVLAN.
PD4-749280880	Installing firmware fails and displays the following message: `tftp: server says: Wrong TFTP State`
PD4-1300795581	IP Fragmentation is not happening with jumbo frame enabled.
PD4-1135195907	With 4,000 VPLS instances, L2 unicast traffic recovers 8 to 10 minutes after disabling and enabling VPLS or MPLS traffic in a three node configuration.
PD4-465744039	ACL counters are not hitting the IGMP packets.
PD4-506754505	When creating a dynamic egress ACL to deny all traffic, the traffic still hits the ARP reply counter but not denying the packets.
PD4-450852442	When configuring an ACL and using the keyword `denyAll` in the `create access-list` command, the action is not stopping the ARP reply packets.
PD4-614541490	VPLS traffic stops after configuring MAC limit-learning.
PD4-720906222	Performing a save and reboot on a DUT with 5,000 dynamic ACLs causes one module to go into a failed state while the remaining modules stay in ACL sync even after one hour.
PD4-690958111	After running the `unconfigure switch all` command, an I/O module may stick in the booting state, resulting in the switch continually rebooting.
PD4-631700490	When PIM and PIM snooping are enabled on the same VLAN, and if that VLAN happens to be a PIM egress VLAN, traffic forwarding does not happen on the VLAN.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description

PD4-973196600	The following error or warning messages are seen after installing firmware from CR 21 (ExtremeXOS 12.3.2.5) to CR 22 (ExtremeXOS 12.4.1):
	`* (debug) BD-20808.8 # show log sev err < Erro:Kern.Error > MM-A: ide0: unexpected interrupt, status=0xd0, count=1`
	`<Erro:Kern.Error> MM-B: ide0: unexpected interrupt, status=0xd0, count=1`
	`<Erro:HAL.Card.Error> MM-A: PHD EEPROM READ ERROR..SLOT=8, ADDR=167`
	`<Erro:HAL.Card.Error> MM-A: Previous message repeated 2 additional times in the last 60 second(s)`
	`< Crit:HAL.Fabric.Critical> MM-A: pioneerBringDownFE200 Bringing Down FE200 on XBAR 2 as the command EXTRUC_FE_MCAST_WRITE_CMD Failed, Reason: UCPIPE_TIMEOUT`
	`<Erro:HAL.Card.PowerStateError> MM-A: A request to power down slot 8 failed - returning a completion code of -1 .`
	`<Erro:HAL.Card.Error> MM-A: PHD EEPROM READ ERROR..SLOT=5, ADDR=167`
	`<Erro:HAL.Card.Error> MM-A: Previous message repeated 2 additional times in the last 59 second(s)`
	`<Crit:DM.Critical> MM-B: Slot-5 FAILED (6) IO Slot5 Micro controller was reset. Attempt to recover`
	`<Crit:DM.Critical> MM-A: Slot-4 FAILED (6) IO Slot4 Micro controller was reset. Attempt to recover`
	`<Crit:cm.file.openErr> MM-B: Failed to open file "/config/primary.cfg": No such file or directory`

PD4-854675001, PD4-860561781	A BlackDiamond 20808 switch with a single MM running ExtremeXOS 12.3.2 software fails to upgrade during a firmware upgrade process. It also fails during the firmware downgrade process. You may need to try and install the firmware multiple times.
PD4-552222911	DUT is hanging with a busy message (dots) after configuring 7,250 ingress dynamic ACLs with conduit errors.
PD4-757707981	Proxy ARP does not work in a PVLAN.
PD4-526514731	On a BlackDiamond 20800 series switch, the system experiences a random packet drop from the MM to the packet processor health check loopback interface.
PD4-730820249	If a route prefix in a BlackDiamond 20800 series switch is more than 24, only 100,000 routes are stored in the hardware. For the route prefixes less than 24, then 512,000 routes are stored in the hardware.
PD4-734160880, PD4-697230006	Extreme Networks does not support the same (S,G) stream entering a switch through multiple constituent VLANs of a private VLAN or VLAN aggregation. If a source moves from one constituent VLAN to another, run the `clear igmp snooping` command.
PD4-1048824150	Deleting meters reports an error after an access list is configured and unconfigured multiple times. **Workaround:** Configure another meter.
PD4-1066604251	In dual MM systems, whenever a meter deletion results in a timeout, the `show meter` command output still shows the meter, even though the error `meter could not be found` is displayed. **Workaround:** Create and use another meter.
PD4-1064653511	The error `.....***** Process hal pid: 474 died with signal:11` is displayed on an active MM when 1,000 policy files are configured on multiple egress ports. **Workaround:** Configurations exceeding the scaling limit are not supported.
PD4-1064653532	When configuring an access list with traffic queues, with a 10G port as one of the egress port, traffic is lost when the corresponding 10G I/O module is hot swapped. **Workaround:** Disable and re-enable the I/O module.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1056439342	I/O modules reboot when egress rate shaping is configured above 1,000 traffic queues with all egress ports. **Workaround:** Configure egress rate shaping with the proper scaling limits.
PD4-861903959	When the backup MM is not yet synced (because of `run msm-failover` or running diagnostics) and one performs an MM-failover, the command is accepted, however, both MMs will then reboot. **Workaround:** Make sure that `run-time diagnostics` command checks that both MMs are in sync before running the diagnostics.

PD4-847978862	A monitor port does not come up after enabling a port after a DUT is rebooted with a disabled monitor port. The following error is displayed while rebooting:
	`MM-A: voyagerCardPowerEnabl`
	`e:1144:- Invalid System mode information returned from dm.`
	`dmGetSystemMode`
	`() = 33`
	`08/15/2009 16:47:02.47 < Erro:HAL.Card.Error > MM-A:`
	`voyagerCardPowerEnabl`
	`e:1144:- Invalid System mode information returned from dm.`
	`dmGetSystemMode`
	`() = 33`

PD4-803757411	Configuring a meter on a BlackDiamond 20808 switch to limit broadcast or multicast traffic (rate-limit flood-traffic) is not possible without an HQoS license.
PD4-748388236	Egress rate shaping does not work after running the `save` and `reboot` commands if an egress port is not specified. Configured egress rate-shaping does not work on a newly inserted I/O module if an egress port is not specified. **Workaround:** Unconfigure the ACL and re-apply the same ACL.
PD4-715473099	The multicast traffic receive rate for 10,000 multicast groups takes an excessive amount of processing time.
PD4-756263261	The `show fabric` command in an ExtremeXOS environment shows the fabric information is XFM-2.
PD4-728354005	On a BlackDiamond 20808 switch, running the `show tech-support` command when I/O modules or fabric slots are in the process of booting, or are otherwise not operational, may cause `sys-health-check` output to display fabric link faults, when there are actually none. This is a transient state. Once the modules are operational, only actual fabric link faults are displayed in the command output.
PD4-603229266	A slot reboots when load sharing is disabled and MVR is disabled and re-enabled.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description

PD4-587169451	Running the `install firmware` command may generate numerous error messages in the Event Management System (EMS) logs. These messages do not impact system performance.
	`<Erro:HAL.Sys.BackupPFCFailed> MM-A: Backup Power Fan Controller (#2) has failed`
	`<Erro:EPM.Upgrade.Fail> MM-A: Upgrade failed, script: install bootrom failed`
	`<Erro:HAL.Sys.GetPFCMastershipFailed> MM-A: Failed to get Power Fan Controller Mastership for slot #17`
	`<Erro:HAL.Sys.OtherPFCFailed> MM-B: Power Fan Controller in slot 17 has failed to communicate with EXOS`
	`<Erro:HAL.Sys.SetBackupPFCToMaster> MM-B: An error happened and is now setting the backup Power Fan Controller #2 to be the master Power Fan Controller`
	`<Erro:HAL.Sys.MasterPFCFailed> MM-B: Master Power and Fan Controller (#1) has failed`
	`<Crit:HAL.Fabric.Critical> MM-A: pioennerBringDownFE200 Bringing Down FE200 on XBAR 1 as the command EXTRUC_FE_READ_CMD Failed, Reason: UCPIPE_ERROR`
	`<Erro:HAL.Sys.Error> MM-A: Slot XBAR1: 23918 FE 0 read 0xb50`

Summit Family Switches	
PD4-1545964372	On a Summit X480 switch, the log message `Setting hwclock time to system time, and broadcasting time` is frequently displayed.
PD4-2094910917	An LDAP bind fails after a system reboot.
PD4-2026467027	When a Summit X670V-48x switch with a 40G port in partition mode connected to a 10G port using MTP breakout cables, the 10G side shows the link is up.
PD4-1950680298	On a Summit X670V-48x switch, inserting a copper GBIC (1000BASE-T) in a 10G capable port changes the speed and duplex setting of the port.
PD4-1996237147	On a Summit X670 switch, the power fan controller is not disabled when using the disable command with the all option.
PD4-2093228351	On a Summit X670 series switch, FDB identities are not flushed from the identity management table.
PD4-2095792132	When clearing an FDB entry or updating a policy entry on VM-tracking, MAC addresses with a wide key policy installed results in the policy being uninstalled. When this occurs, the following error message is displayed: `ACL filter install failed on vlan *, port 1:16, rule "VM1:16_00:00:11:00:00:1a_E601" index 601, Invalid parameter (user-defined field (UDF))"`
PD4-1824530443	The following behavior differences were observed between a Summit X480 and a Summit X450a switch: • Configured a general query interval of 125 seconds but a Summit X480 switch sends general queries every 130 seconds. This issue is not seen on a Summit X450a switch. • A Summit X480 is sending both MLDv1 and MLDv2 reports even though only MLDv2 is enabled. This issue is not seen on a Summit X450a switch.
PD4-1436226210	With default ethertype (0x88a8) configured, Summit X460 and X480 switches do not display an error message when adding a port as tagged to a VMAN when the port is already part of a tagged VLAN. When the port is already part of an EAPS control VLAN, EAPS goes to a failed state.
PD4-1721719301	The process HAL crashes with signal 11 after configuring a primary and secondary pseudo wire and sending unicast traffic through the pseudo wire.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1676631313	When disabling sharing on a load-shared port that is part of multiple VLANs, VLAN statistics shows a "-" for some VLANs. **Workaround:** Unconfigure and reconfigure VLAN statistics.
PD4-1659644826	VLAN statistics monitoring is unconfigured for a specific VLAN if the VLAN name is changed.
PD4-1648023331	A Summit family switch configured with MLAG does not reply to the first ARP request received on an ISC port.
PD4-1664831900	VLAN statistics are included in the output of the `show configuration` command for load-sharing member ports even after the `unconfigure ports monitor vlan` command is issued. **Workaround:** Disable sharing, remove the VLAN statistics configuration, and enable sharing.
PD4-1673106807	For certain match conditions involving SIPv6 and DIPv6, packets may not hit an ACL in a Summit X450a switch.
PD4-1676631313	When disabling sharing on a load-shared port that is part of multiple VLANs, VLAN statistics shows a "-" for some VLANs. **Workaround:** Unconfigure and reconfigure VLAN statistics.
PD4-1637091230	With 4,000 VPWS sessions, traffic recovery takes approximately 8 minutes before a port flap occurs. **Workaround:** On a Summit X460, it is recommended that you only configure 1,000 VPWS instances.
PD4-1589959110	When adding ECMP routes using OSPF, a route flap occurs.
PD4-1590249340	Clearing FDB entries when a Summit X480 switch learns 512,000 MAC addresses from MLAG ports disrupts MLAG peer TCP sessions.
PD4-749682632	You cannot run the `configure port auto on` command on XGM2-2bt ports.
PD4-427423116	When a dot1x client is authenticated at multiple VLANs, the output of the `show netlogin port` command shows the client is sometimes authenticated at the local server and other times at a RADIUS server. **Note:** This occurs when dot1x and MAC authentication are enabled on the port.
PD4-1142692318	On Summit X480 switches, L3 multicast traffic sent from a service VLAN/VMAN to VPLS is not received at the VPLS peer. **Workaround:** When VPLS enabled VLANs exist on a port, all VLANs on that port must have IGMP snooping disabled. Also, the IP address cannot be configured on any other VLANs (including non-VPLS VLANs). Remove ports from the default VLAN.
PD4-448681226	The `show l2stats` command does not count ARP packets to the CPU, even though the packet goes to the CPU.
PD4-489142320	One Gigabit ports set to `auto on` flap twice during a switch reboot.
PD4-489359602	Conflicting Link Fault Signal (LFS) alarms are shown when disabling local ports.
PD4-274249122	If a Summit switch populated with an XGM2-2bt module is rebooted, a false link up is seen on 10G links connected to the XGM2-2bt ports approximately 30 to 50 seconds before the switch has fully booted.

PD3-43606168	If sFlow does not have a collector configured using the `configure sflow collector` command, the `show log` command generates the following messages:
	`08/23/2005 12:28:09.55 <Noti:sflow.debug.AddCntSmplFail> : Could not add the counter sample for port 0:1020, as receiver is not configured.`
	`08/23/2005 12:07:49.55 <Noti:sflow.debug.AddCntSmplFail> : Previous message repeated 61 additional times in the last 1200 second(s).`

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-40266236, PD3-40233121	Traffic on load share ports configured as redundant ports incorrectly moves to other ports in the load share group during link transition.
PD3-202013281	Learning is disabled by default on remote mirroring VLANs. Running the `enable learning` command on those VLANs may cause a loss of remote mirrored traffic.
PD3-202013298	The valid value range for tags on remote-mirroring VLANs is 1 to 4,094. Use these values for configuring the remote tag in the `enable mirroring` command.
SummitStack	
PD4-2234586031	When using a SummitStack, known L2 traffic sent to port 64 is not forwarded in 4x10G mode.
PD4-1992180351	A Summit X670 stack does not provide details for the VIM4-40G4x module shown in the output of the `show version` command.
PD4-1678164933	After upgrading to ExtremeXOS 12.5.1.4, the following error is shown in the log: `<Erro:Kern.IPv4Mc.Error> Slot-1: Unable to Del IPmc vlan 924 for 1:15 s,G=a9e6f05,e1010028 IPMC 186, unit 0 Entry not found.`
PD4-1645865216	The following error message is seen when operating a stack where the backup switch does not have the same feature pack licenses as the master switch. `Error: Backup execution timed out, command execution aborted!` **Workaround:** When using VRs, be sure that while forming the stack using mixed platforms, the master node and backup node have the same licenses feature pack.
PD4-1655280966	Using a SummitStack, a system crash may occur after running the unconfigure mpls command and then loading scripts to configure MPLS. **Workaround:** Use the CLI to configure MPLS line by line. Do not use scripts to load a large MPLS configuration.
PD4-928567091	Running the `synchronize` command on a Summit X650 in a SummitStack causes the system to time out and the stack to not synchronize for an extended period of time This also results in the master node no longer being accessible.
PD3-181304741	After inserting a XENPAK in a stack (XGM2-2xn, XGM-2xn) and performing an snmpwalk on the entityMib entPhysicalDescr variable, XGM- is always shown, not the complete module description.
PD3-209191768	After running the `disable port all` command on a SummitStack, some port LEDs may sometimes light green even though ports are not up.
PD3-204744742	IPv6 neighbor-discovery in a management VLAN in a SummitStack resolves to the node address of the stack master, instead of the stack MAC address.
PD3-136493921	If a switch is added as a master-capable node of a stack whose master node has a license level that is not equal to the level of the switch, the switch will fail. The complete condition can be seen using the `show slot detail` command. In this state, the switch does not have AAA services available. You will only be able to log into the switch using the failsafe account that was last assigned to it. You must log into the switch to upgrade the license. If the switch is not using the failsafe account configured on the stack, you can use the `synchronize stacking {node-address <node-address> | slot <slot-number>}` command to copy the failsafe account information from the master switch to the failed switch NVRAM. You can also use the `configure stacking license-level` command to configure a license level restriction on the entire stack and then reboot the stack. Once the stack is restarted, there is no longer a license mismatch, enabling you to log into the switch and upgrade the license. From the master switch, run the `unconfigure stacking license-level` command to get the stack to operate at the desired license and then reboot the stack.
BGP	

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-2095378160	BGP crashes with signal 11 when receiving updates from an IBGP peer, which in turn receives updates from a third party EBGP peer.
PD4-2096016911	On a Summit X670 series switch running alternate stacking, L2 and L3 known traffic is not forwarded across slots for port 32-44.
PD4-2099675994	BGP traffic drops when a route switches from IBGP to EBGP when terminating BGP on peer switch.
PD4-1639664566	With graceful restart enabled and import-policy set, BGP routes are withdrawn from the adjacent peer after restarting process BGP (routes are re-advertised to adj only after grace period expires).
CLEAR-Flow	
PD4-278443631	CLEAR-Flow commands display on platforms that do not support this capability, including the Summit X150, X250, X350, and X450e series switches, as well as BlackDiamond 8800 non-c-series switches.
EAPS	
PD4-1909431762	The `debug eaps check configuration` command does not return a warning if a VLAN is not protected but has EAPS ring ports.
PD4-1673032272, PD4-1676753651	EAPSv2 segment health-check packets received on a ring port may be dropped if the EAPS node on a Summit family or BlackDiamond 8800 series switch has a different EAPS shared port on any other ring ports.
PD4-749215481	Disabling the EAPS master primary port when there are no other ports configured on a protected VLAN will cause a disruption of L2/L3 multicast traffic. **Workaround:** Enable loopback on all EAPS protected VLANs.

PD4-471892924	Restarting the EAPS process on a controller generates the following error messages on a console, but does not impact switch performance.
	`BD-8806.80 # restart process eaps`
	`Step 1: terminating process eaps gracefully ...`
	`Step 2: starting process eaps ...`
	`Restarted process eaps successfully`
	`BD-8806.81 # ERROR:VmgrProtocolIfRegister protoId:0 numIf:1`
	`ERROR:VmgrProtocolIfRegister protoId:0 numIf:3`
	`ERROR:VmgrProtocolIfRegister protoId:0 numIf:1`

IP Routing Protocols	
PD3-39411271	icmpInMsgs counter will display the incoming ICMP packets for VR-Default only.
PD3-128093864	MSDP Source-Active responses received from non-RPF peers are not processed.
PD3-192821161	For Summit X650, X450 a-series and e-series switches, and the BlackDiamond 8800 series of switches, the maximum number of supported IP interfaces is 512 (IPv4 and IPv6 combined). If there are more IP interfaces configured, the following log message is displayed: `<Info:HAL.VLAN.Info> Maximum # of IP interfaces (512) already configured. Could not add IP address 0x0A010101 mask 0xFFFFFF00`
PD3-202580681	Enabling IP route compression may cause temporary slow path forwarding for some of the L3 traffic.
PD4-718946965	Directed broadcast traffic is not being forwarded.
Mirroring	
PD3-79867211	If you create a load sharing group (trunk), then enable mirroring to a port, the software allows you to add the mirroring port to the load sharing group.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
MPLS	
PD4-1992679531	In VPLS, when configuring 7,190 pseudo-wires, FDB entries are not learned on 100 pseudo-wires.
PD4-1592270405	The `run msm-failover` command shows the following warning message in the log. `<Warn:Kern.IPv4FIB.Warning> Slot-4: dest 0x0A9E6D7C / 30 nexthop 0x0A9E6D39: Unable to add route to unit 1, rc Entry exists. Shadow problem.`
PD4-464587012	All unicast traffic routed by MPLS is stopped when penultimate hop popping (PHP) is enabled on all MPLS VLANs. VPLS traffic is not impacted.
PD4-475414370	The following warning message is seen numerous times after changing VLAN Virtual Private LAN Services (VPLS) mappings: `<Warn:MPLS.LDP.InternalProb>`
PD4-475414505	In more complex topologies, detour Label Switched Path (LSP) connections are not set up.
PD3-157687121	ExtremeXOS software uses Control Channel Type 2 to indicate router alert label mode. In MPLS Router Alert Label mode, VCCV packets are encapsulated in a label stack. However, the existing VCCV packets are sent like a stack without any PW label.
PD3-184989177	When an `LDP advertise static` setting is set to `all`, all static routes are treated as egress routes and egress LSPs are created. That is, a label is generated and advertised for the static route. If the router at the end of the static route advertises a label matching that static route, the LSP that was previously an egress LSP becomes a transit LSP. An ingress LSP should also be created whenever a label is received, however, the ingress LSP is never created. **Workaround:** Do not use the `LDP advertise static all` configuration in situations where an ingress LSP for a static route is required.
PD3-139423053	Running the `show mpls rsvp-te lsp summary` command on a system configured with 2,000 ingress LSPs takes an excessive amount of time to process.
PD3-92653036	The `show mpls label`, `show mpls rsvp-te label`, and `show mpls rsvp-te lsp` command output currently does not display egress LSPs using advertised implicit NULL labels.
PD3-111544904	When a router receives an explicit NULL label, it is incorrectly treated as an implicit NULL label, so rather than sending label 0, no label is sent.
PD3-93218551	If either an egress or a transit LSP traverses the system, and an MPLS labelled packet containing a router alert label is received, that packet is not forwarded.
PD3-93069318	Only VLANs configured as protocol *any* should be added to MPLS.
PD3-104731701	When a traceroute is performed by setting the MPLS TTL to the IP TTL, ExtremeXOS does not correctly send back an ICMP response. The result is "*" characters in the traceroute for the routers that timed out. If a route is available, ExtremeXOS should attempt to send back an ICMP response.
PD3-93630853	LDP should not advertise a label mapping for a direct VLAN that does not have IP forwarding enabled.
PD3-203917264	When an explicit route object (ERO) is changed for an LSP session that is up, the LSP that is already up is not torn down. LSP stays up based on the older values. The retry count continues to increment as LSP tries to come up with new values by querying routes every 30 seconds. This is done while the earlier LSP session is still active using the previously configured values. See the retry count in the command output for the `show mpls rsvp-te lsp <lsp_name> detail` command.
Multicast	
PD4-1375779464	In the output of the `show ipstats` command, the first packet of a multicast stream is incorrectly counted up as `discards` in the router interface.

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-581950231	Multicast traffic is not received even though the rendezvous point (RP) tree and source information is shown in the PIM cache table
PD4-521915271	The Internet Group Management Protocol (IGMP) group reports may occasionally change from Version 2 to Version 3.
PD4-339945634	When a load-sharing group is a member of a mirrored VLAN, packets ingressing on the member of the load-sharing group in the mirrored VLAN should be mirrored. On the Summit family switches and BlackDiamond 8800 modules, packets ingressing on member ports other than the master port of the load-sharing group in the VLAN are not mirrored. **Workaround:** Packets ingressing non-master ports in the load sharing group on the mirrored VLAN can be mirrored by adding virtual port mirroring filters for each of the non-master member ports.
PD3-78144711	The `show ipstats` command does not increment IGMPv3 statistics.
PD3-79383551	IGMPv3 Report Record type "5" does not work as expected when sent after a type "2" or a type "4" message.
Network Login	
PD4-468366251	A network login client is not authenticated if the username is 32 characters. Only 31 character user names are supported, even if the user can create a 32-character username.
PD4-763062511	Hitless upgrade is not supported for network login in ExtremeXOS 12.3.1.
PD4-752731351	You should not be able to enable network login if a VLAN is a VLAN-aggregation Sub VLAN. The system should generate a syntax error.
Network Services	
PD3-93829391	Configurations using a VR-Mgmt interface as a RADIUS client IP may not load at boot-up. However, using an interface in VR-Default will load correctly.

PD3-67727590	Creating two sets of VMAN ACLs with 4000 entries each and performing a VMAN ID translation on each ACL may generate the following error:
	`.....03/15/2006 17:57:28.84 <Info:pm.config.openingFile> MSM-B: Loading policy RLL20k from file /config/RLL20k.pol`
	`...03/15/2006 17:57:32.46 <Info:pm.config.loaded> MSM-B: Loaded Policy: RLL20k number of entries 4002`
	`.........Error in alloc txmi txmi 0x9f2 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x9f4 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x1102 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x9f6 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x9f8 txmdi 0xffffffff`

OSPF	
PD4-2078865382, PD4-1493257018	The forwarding address in an external LSA should not be set for an interface that is configured as passive.
PD4-1641495299	When 5,000 routes are received via the OSPF neighbor and advertised to 253 neighboring OSPF routers, all 253 sessions go down. It then takes nearly 20 minutes for the sessions to come back up.
PD4-1548969848	OSPF neighbors remain in the Exchange state after disabling and enabling an OSPF instance.
QoS	
PD3-67431351	Configuring an ingress traffic queue and an egress traffic queue association to multiple ports in sequential order generates the following error: `Egress queue already associated to this ingress queue Configuration failed on backup MSM, command execution aborted!`

Table 38: Open Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-16578296	The member ports of a trunk will retain the QoS profile configuration of the trunk (based on the master port) after load sharing is disabled, or if a port is removed from the trunk.
RMON	
PD3-12950492	Issuing the `clear counter` command might cause a high number to be displayed in variables such as etherHistoryOctets, etherHistoryPkts, and etherHistoryTable.
ScreenPlay	
PD3-111344472	ScreenPlay allows you to configure DHCP but you cannot enable DHCP.
Security	
PD3-205012219	The source IP lockdown dynamic deny ACL counter is not working properly and increments valid traffic from a trusted client.
PD3-186939931	Ingress mirroring is not working for DHCP snooping when snooping is enabled on BlackDiamond 12800 series switches. DHCP snooping works correctly when DHCP snooping is disabled.
PD3-75120608	The `unconfigure radius` and `unconfigure tacacs` commands do not reset the timeout value to the system default of 3 seconds.
SNMP	
PD4-2189652914	SNMPv3 privacy with AES128 is not working.
PD4-1859776249	A switch resends SNMPv3 Inform Requests even after an SNMPv3 Inform Response is received from an Inform receiver.
PD4-1388191921	When changing an SNMP master configuration using SNMP set, the changes are not immediately reflected in the `show configuration snmp` command output. **Workaround:** Run the `save configuration` command to see the changed configuration in the `show configuration snmp` output.
PD4-705730556	AES/3des users created using ExtremeXOS 12.3.1 software cannot be used for SNMP operations in ExtremeXOS 12.1 or earlier releases. This may cause the SNMP master to crash.
Spanning Tree Protocol	
PD3-189927343	A temporary loop occurs when a root bridge is taken down by disabling all ports or powering down the switch.
UPM	
PD4-1664927541	UPM profiles for events identity-detect and identity-undetect are not executed when many unique kerberos users login simultaneously from two client PCs. This happens when 50 unique users login continuously from PC1, and another 50 unique users login continuously from PC2 at the same time.
WAN PHY	
PD3-101226461	When `show wan-phy` commands are run on non WAN PHY ports, the ports display the headers. It should only display the error `wan command is not supported on non-wanphy port 25`.

Known Behaviors

The following are limitations in ExtremeXOS system architecture that have yet to be resolved.

Table 39: Known Behaviors, Platform-Specific and Feature PDs

PD Number	Description
BlackDiamond 8800 Series Switches	
PD4-2066740891	After rebooting a BlackDiamond 8800 series switch with a dual MSM, files are not downloaded to `/tmp/vmt` until unconfiguring and reconfiguring the vm-tracking repository.
PD4-2066401919, PD4-1323337297	A switch experiences memory depletion because of the HAL process when sending L2 traffic to a PVLAN with a continuous SA increment.
PD4-901339876	IdMgr should immediately flush kerberos entries when a port goes down and not wait for the kerberos snooping time to expire.
PD4-1911293840, PD4-1858470951	CLI sessions hang when executing the `show port <port-num> transceiver information detail` command while snmpwalk is running.
BlackDiamond 12800 Series Switches	
PD4-1922513168	EPM process crashes with signal 6 when upgrading a switch from ExtremeXOS 12.2.2 to ExtremeXOS 12.3.5 when an SSH license file has 100 or more SSH licenses.
BlackDiamond 20800 Series Switches	
PD4-1285717901	With 15 ports in a LAG, the maximum to minimum bandwidth utilization difference between ports is 21%. With 16 ports, bandwidth utilization is 8%.
PD4-1644777015	The internal QoS profile selected for a packet leaving the Provider Backbone Bridged Network (PBBN) is derived from the 802.1p bits of the B-tag in the packet.
PD4-1571801812	When a mirroring-to port is a LAG, load sharing is done only based on the mirror header and not on the configured LAG algorithm.
Summit Family Switches	
PD4-1592270392	A Summit X480 stack may get stuck in the backup state after running the `show switch` command after a system reboot or failover.
PD4-1679504312	A Summit X460 switch crashes when MSTP is configured with 64 MSTIs and 1,000 VLANs.
PD4-1642703687	The VLAN statistics transmit counter does not count the packets matching an egress ACL rule in a Summit X480 switch.

Table 39: Known Behaviors, Platform-Specific and Feature PDs (Continued)

PD Number	Description
ACL	
PD3-77983510	Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series modules provide more powerful ACL capabilities. Because of this, the amount and complexity of ACL rules will naturally impact the time needed to process and apply the ACL rules to the switch. This will also impact switch bootup time. Access Control List limitations fall into two areas: physical and virtual. Physical Limits—Summit X450a and Summit X450e series switches: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1,024 rules for the Summit X450e and 2048 rules for the Summit X450a. Physical Limits—BlackDiamond 8800 a-series and e-series modules: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1,024 rules for the e-series modules, and 2048 rules for the a-series modules. Extreme Networks recommends that you configure ACLs as per-VLAN, wildcard, or single-port. If either of the following is true, you will have to configure ACLs with multi-port lists: Your application requires that ports do not have a homogeneous ACL policy. When BlackDiamond 8800 original series modules are operational in the same chassis, it may be necessary to configure ACLs to specific port-lists instead of as wildcard or per-VLAN. This is because the original series modules have smaller physical limits. Virtual Limits—Summit X450a and Summit X450e series switches: When configuring a multi-port ACL, use the following guideline. The total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules. For example, applying a 1,000 rule policy file to a 48 port multi-port list is supported (1,000 rules * 48 ports in the list <= 48,000). Virtual Limits—BlackDiamond 8800 a-series and e-series modules: When configuring a multi-port ACL, use the following guideline. For any a-series or e-series blade in the system, its total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules. For example, applying a 1,000 rule policy file to a 48 port multi-port list on an a-series module on slot 1 and an e-series module in slot 2 is fine. Neither module exceeds the 48,000 total ACL rules. Excessive boot times and CPU resource starvation can be seen with larger total rule counts. If your application requires additional capacity, contact Extreme Networks.
BGP	
PD4-1618725742	A BlackDiamond 20800 series switch with 100 egress VLANs crashes when multicast traffic for 1,000 (S,G) entries is received in a burst with varying packet sizes.
MPLS	
PD4-452308541	The secondary pseudowire on an ESRP master switch does not take the secondary switch node pseudowire after the primary switch is rebooted.
PD4-476351932	Performing a `restart process mpls` or `restart process ospf` on a spoke node in an HVPLS setup causes the Label Distribution Protocol (LDP) peer to go down with the core node. **Workaround:** Disable and enable MPLS.
PD4-475414558	Changing a Label Switch Router (LSR) ID causes all Label Distribution Protocol (LDP) peers to go into a NonExistent state.
Network Login	
PD4-1653484241	Network login cannot authenticate MAC addresses on more than 10 VLANs.

Resolved Issues in ExtremeXOS 12.6.2-patch1-9

The following issues were resolved in ExtremeXOS 12.6.2-patch1-9. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 40: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2630598093	CPU utilization of `snmpMaster` process goes up to 99% when SNMPv3 access is disabled and the `rmon` rule is set.
BlackDiamond 8800 Series Switches	
PD4-2635892931	In BlackDiamond 8800 series switches, using a customer configuration, the I/O module takes more than 92 minutes to go to operational state.
Summit Stack	
PD4-2637502930	In Summit Stack, when CPU-generated packets are sent to an egress port which transits through an x670, x440, or 40G VIM module, tag 0 is added to that packet.
Summit Series Switches	
PD4-2611913461	When a peer connected to an X670-48x is rebooted, ports on the X670-48x can remain struck in the down state. This is an intermittent timing-related issue, it does not appear with every reboot, and it occurs only on a few devices.

Resolved Issues in ExtremeXOS 12.6.2-patch1-8

The following issues were resolved in ExtremeXOS 12.6.2-patch1-8. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 41: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2616260135	When Super VLAN and Sub VLANs are configured, DHCP offer messages are sent out with incorrect tag values.
PD4-1842342815	When working in network login, after a dot1x client logs out, the port is not moved to a MAC-based VLAN.
PD4-2623268792	The UPM timer is drifting when configured with sntp-client.
PD4-2627768059	When timezone ends with the number, it takes a number as an offset.
PD4-2634400745	After establishing 8 active SSH connection to the switch, the connection terminates after 60 minutes and subsequent SSH connections are rejected with an error message like the following: `"Maximum number of shell sessions has been reached".`
PD4-2587119536	The `xmld` process dies while closing the `xml` session.

Table 41: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-2579506802	Installing and uninstalling `xmod` in non-active non-selected partition changes the selected image configuration.
PD4-2488933836	In VMAN, access-list modifiers **`mirror-cpu`** and **`log`** are not working.
PD4-2444973765	Packet duplication occurs if a remote-mirroring VLAN is present in the switch after the following issuing the CLI command **`disable/enable learning port`**.
PD4-2627584891	After creating the meter, the command **`show meter`** does not show the meter name when doing a “tab” or “?”
PD4-2595913311	Packet IDs for RADIUS Authentication are not timing out if an Access-Accept, Access-Reject, or login timeout is not received.
PD4-2623732931	FDB entries are not being learned in VPLS if the MPLS LSP takes different path in opposite directions.
PD4-2623732970	MPLS entries not getting programmed in hardware causing VPLS traffic loss.
BlackDiamond 8800 Series Switches	
PD4-2631983036	With EXOS/8900 (G96Tc) IO modules, ACL installation fails when using more than 32 LAG ports.
PD4-2618280391	In a VPLS instance, if MPLS LSP takes different path in opposite directions, then broadcast packets might be dropped and not forwarded to the service VLAN.
PD4-2635893288	In BlackDiamond 8900, L2 unicast packets are being flooded even though the destination MAC is present in the FDB table.
PD4-2600494631	dhcp-snooping does not show the client port on Sub VLANs, and dhcp-bindings are shown only on Super VLANs.
PD4-2589012113	Unable to ping the DHCP-Server from DHCP Client when configured with the CLI command **`enable ip-security arp validation ip`**.
PD4-2616151804	In BlackDiamond 8900, Bootprelay breaks after removing a port from the Sub VLAN when the port is part of the VPLS service VLAN.
Summit Stack	
PD4-2582145318	A HAL error occurs on reboot of a switch with a load-sharing configuration.
PD4-2579829417	Fetching Stack Detail Fails in Screenplay.
SNMP	
PD4-2317279376	SNMPv3 user password is changed after loading the ASCII-formatted configuration file.
PD4-2582033086	SNMP community strings are visible to user level accounts.

Resolved Issues in ExtremeXOS 12.6.2-patch1-6

The following issues were resolved in ExtremeXOS 12.6.2-patch1-6. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 42: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2462471211	Summit X460-24x fan RPM gives out-of-range errors.
PD4-2493634822	In PVLAN, configuring multiple ports as the loopback-port for subscriber VLAN should be blocked.
PD4-2550962536	The switch goes into a reboot loop if two dynamic ACLs are attached to a port which already has ACL policies applied on it.
PD4-2527280688	When mirror-cpu action with log is used in the access list policy file, CPU-bound traffic is not logged.
PD4-2527617689	The CLI command **`enable ssh2 access-profile none`** does not take effect unless the `ssh` process is restarted.
PD4-2485926270	In Extreme XOS 12.6.2 /Summit Stack: ELRP configuration fails after failover on the new Master node. The issue happens after unconfiguring an ELRP client and attempting to again configure the ELRP client.
PD4-2526240871	When too many messages need to be logged, the emsServer crashes with `signal 11`.
PD4-2532423697	In Summit platforms and BlackDiamond 8800 Series Switches, FDB learning does not happen and the log files show the following error: `12/24/2011 08:57:12.38 <Erro:HAL.Card.Error> MSM-A: pibConduitRcvMsg: no magic number (0x8001) slot number 9, tcp port 5002`
PD4-2555520846	An SNMP request on extremeEapsState returns an empty result after a reboot.
PD4-2522108546	A slow memory leak occurs in the VLAN module during SNMP polling from Ridgeline.
BlackDiamond 20800 Series Switches	
PD4-2549423721	In BlackDiamond 20800 Series Switches, if the VMAN tagged port receives a single tagged (0x8100) multicast packet, it will be forwarded as a double tagged (0x8100) packet which results in packets being dropped by other switches in the network due to an unexpected tag.
PD4-2478971757	The output of the CLI command **`show access meter ports`** displays an incomplete value in BlackDiamond 20800 Series Switches.

Resolved Issues in ExtremeXOS 12.6.2-patch1-5

The following issues were resolved in ExtremeXOS 12.6.2-patch1-5. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 43: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2501758362	Process `rtmgr` hits 99% CPU during link flap of LAG port in PIM enabled VLAN.
PD4-2503653963	Description for the CLI command **`configure log target syslog all format timestamp hundredths date`** needs to be updated with correct RFC number - 3164.

Table 43: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-2515490179	In some scenarios, even after the `ssh` session is closed, corresponding resources are not freed.
PD4-2514722216	The default configuration for circuit-id port-information on slot 10 appears in **`show configuration ipSecurity`** CLI command output.
PD4-2516934355	**`show configuration non-persistent`** is not displaying any non-persistent CLI configuration commands.
PD4-2516934480	When a switch receives a TCP Syn attack, the message shown in the log is incorrect.
PD4-2489197546	EXOS/IPv4 Route Sharing: In a route sharing setup, when routes are replaced with a new set of alternate routes the nexthops are not updated correctly when the alternate routes are installed.
PD4-2468887959	In EXOS 12.4.3, VLAN names with 32 character are not handled correctly by PIM. Saving the configuration fails with `Error while saving "pimInterface.`
PD4-2487068919	In all EXOS versions, if monitored ECC error counts are beyond threshold value, system-health-check recovery action needs to be taken.
BGP	
PD4-2516913636	In BGP update message, if AS path segment length is less then 255 bytes, then PATH Attribute flag for AS PATH should not be set as Extended.
Multicast	
PD4-2397008813	In the output of the CLI command **`show ipstats`**, the first packet of a multicast stream is wrongly counted up as *discards* of Router Interface.
DHCP	
PD4-2488452266	Duplicated DHCP Offer and Ack packets are observed when configuring ip-security violation-action to none.
ESRP	
PD4-2499426213	MSM failover causes `ESRP Slave` to become `ESRP Master` for short interval of time and then it falls back to `ESRP Slave` state.
EAPS	
PD4-2334676914	The CLI command **`debug eaps check config`** should return a warning if the VLAN is not protected but has EAPS ring ports.
Summit Platforms	
PD4-2383233640	Private VLAN configuration accepts LAG master port as loop-back port.
PD4-2455246227	The `idMgr` process crashes with `signal 11`.
PD4-2471574786	Sync-E (ZL30142) init code needs to exclude Summit X460-48T/24T and PoE variants.
SNMP	
PD4-2523373431	`extremeCurrentConfigInUse` returns the incorrect value (4-factoryDefault) irrespective of `Config Booted`.
ACLs	
PD4-2460215966	When more than 40 rules in the policy file are using the same counter name, the process `hal` dies with `signal 6` after the CLI command **`show access-list counter`** is executed.
PD4-2517084234	When running EXOS 12.5 and 12.6a Summit X450a cannot save or apply dynamic ACLs via Screenplay.
PD4-2502394582	Applying policy without source MAC is resulting in ACL crash with `signal 11`.

Table 43: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-2510614421	Deny ARP ACLs using arp-sender-address as an ACL match condition will result in blocking all CPU bound traffic.
PD4-2488658156	When the ACL policy file is modified by including *counter*, the counter is not incremented after an MSM failover.

Resolved Issues in ExtremeXOS 12.6.2-patch1-3

The following issues were resolved in ExtremeXOS 12.6.2-patch1-3. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.5, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 44: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
D4-2300925487, PD4-2298873324	After upgrading a switch from ExtremeXOS 11.6 to ExtremeXOS 12.3 with a specific configuration, a memory leak occurs in the EMS process.
PD4-2413922905	When TACACS+ is configured to perform command authorization, switching to a user created VR (or even vr-mgmt) causes an AAA process crash with `signal 6`.
PD4-2446669325, PD4-2274696903	Even after disconnecting an SSH session, the last typed CLI command is executed.
PD4-2446669227, PD4-2270172017	When entering the CLI command configure rate-limit flood twice, the following error message is displayed: `Configuration failed on backup MSM, command execution aborted!`
BlackDiamond 8800 Series Switches	
PD4-2420031475, PD4-1623647801	The watchdog timer reboots when FDB entries begin aging out entries with forwarding configured to use only L2 external tables. This only occurs when a chassis contains an MSM-G8X and 8900-G48T-xl combination.
Summit Family Switches	

PD4-2456675926, PD4-1421166009	The Alternate Bootrom Version and Default Bootrom Version shown in the show tech all command output are displayed as unknown.
	`Alternate Bootrom Version: unknown**`
	`Default Bootrom Version: unknown**`

PD4-2375437695, PD4-2126200252	Changing a PVLAN port-type causes traffic to stop forwarding for different PVLANs.
PD4-2440595311, PD4-2005566801	CPU utilization remains at 99% when running the THTTPD process.
ELSM	
PD4-2313793081, PD4-1838462545	When ELSM detects a link down, ELSM does not deactivate the port.
Multicast	
PD4-2446737435, PD4-2136974279	Deleting the secondary IP address of a VLAN not only disables IP forwarding, it also disables IP multicast forwarding. **Workaround:** Disable IP multicast forwarding by unconfiguring the primary IP address of the VLAN.
OSPF	
PD4-2271653883, PD4-2235844842	Using a specific configuration, OSPF neighbors may become a designated router even though the switch only has an Advanced Edge license.
PD4-2302994105, PD4-1159043115	If active ports are added to a VLAN before configuring IP forwarding using the `enable ipforwarding` command, the direct route is not redistributed into OSPF.
SNMP	
PD4-2446737237, PD4-2148690723	When adding an SNMP trap receiver without specifying a VR name, the `show snmp vr <vr name>` command does not display the configured SNMP trap receiver.

Resolved Issues in ExtremeXOS 12.6.2-patch1-2

The following issues were resolved in ExtremeXOS 12.6.2-patch1-2. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.4, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 45: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2330727748, PD4-2080577061	Multicast manager crashes with `signal 6` when receiving an IGMP report or query on a PVLAN.
PD4-2360863155, PD4-2282342480	When using the ExtremeXOS scripting feature, the script variables are corrupted, resulting in a cliMaster process crash.
PD4-2330267903, PD4-2180137391	When running the `enable cli-config-logging` command, some CLI commands are logged even though they did not make any configuration change.
PD4-2397002069, PD4-1137822041	When mirroring is enabled with port-list and a loopback port is disabled, packets are not sent to mirrored ports.
PD4-2314248918, PD4-1180559831	In a PVLAN with a loopback port configuration, L2 unicast traffic does not flow from a network VLAN tagged port on a switch to an isolated VLAN tagged port on a connected switch.
PD4-2330473363, PD4-2012884711	The following critical message may be logged followed by a system crash when making a configuration change to a private VLAN: `System call ioctl failed failed: informCfgVlanAddPorts and 15`
PD4-2303255351, PD4-2193122709	A HAL process crash occurs when running pibConduitSlotHandler.
BlackDiamond 8800 Series Switches	
PD4-2365722181	Calibrating BlackDiamond 8800 series v4 I/O modules timeout when running an ExtremeXOS 12.6 software image.
BlackDiamond 10800 Series Switches	
PD4-2335806678, PD4-1280018491	Running the `show fans` command on a BlackDiamond 10800 switch shows non-existing fans in the command output and generates alarms when encountering fan health check packet drops (ESMI messages).
BlackDiamond 20800 Series Switches	
PD4-2330727681, PD4-1956113857	Protocol-based VLAN support is not available on BlackDiamond 20800 series switch platforms.
PD4-2357758288, PD4-1860744689	The MIB contains a duplicate entry for the object identifier of a BlackDiamond 20800 series switch.
Summit Family Switches	
PD4-2352974642, PD4-2179522691	A Summit x450a-24t switch is unable to upload debug information to a TFTP server if a colon is included in the SNMP system name if the switch is running ExtremeXOS 12.4.1.7 and 12.5.3.9.
PD4-2330727843, PD4-1600530241	A HAL crash with `signal 11` occurs when connecting a ReachNxt device to a load-shared port. **Workaround:** Do not connect a ReachNxt device to a load-shared port.
PD4-2360863012, PD4-1828079231	A Summit X480 crashes when trying to configure a Sub VLAN.

Table 45: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-2415630995, PD4-1416734218	ICMPv6 packet received by Summit series switches such as the Summit X460, X480, and X650 are sent to the CPU and are duplicated while forwarding to ports in a VLAN.
PD4-2352397589, PD4-2360872231	On a Summit X480 series switch, source MAC addresses are not re-learned after the FDB age-out period.
PD4-2397754647, PD4-2353166279	PoE stacking on a Summit X460 switch is unstable and leads to slot failures. This occurs when all PCs connected to the stack are turned on.
PD4-2321693764, PD4-2193122757	The syslog format on a Summit X450e series switch changes before and after rebooting the switch.
PD4-2271743894, PD4-2271743771	A Summit X650 series switch is showing `smbus_wait _rdy` error messages causing the switch to hang.
PD4-2374597505	On a Summit X670 series switch, multicast entries are not refreshed even with continuous multicast traffic.
SummitStack	
PD4-2410915431, PD4-1603951551	On a Summit X460 stack, the following kernel warning is seen in the log during a failover. `<Warn:Kern.Card.Warning> Slot-1: select_mux:line 250:I2C I/O operation failed`
PD4-2396286645, PD4-1527290887	In a SummitStack, when an external PSU is powered on/off, the wrong log message is displayed.
PD4-2385033386, PD4-1451573201	When rebooting a SummitStack switch, the following warning message may be displayed: `hal: page allocation failure. order:9, mode:0xd0`
ACL	
PD4-2341851142, PD4-2338323749	With a specific combination of ingress and egress ACLs, traffic is not blocked as expected.
DHCP	
PD4-2365940869, PD4-2202931730	When an IP security violation action is set to drop-packets, DHCP NAK packets are dropped on DHCP trusted ports.
EAPS	
PD4-2312036214, PD4-2014131056	If a port state is set to preforwarding, when a shared port is down and the link flaps between another two nodes with traffic, the flap results in traffic loss for 15 seconds.
PD4-2345807021, PD4-1991277241	If an untagged service VMAN port is also an EAPS ring port, the EAPS control packets received on the EAPS ring port are not getting copied to the CPU. Also, EAPS control packets are being sent via an untagged service VMAN tunnel, instead of flooding to other EAPS ring ports on the EAPS control VLANs.
PD4-2338323205, PD4-2027694734	Running the `debug vlan show vpifs <vlan> <port>` command returns the incorrect state for an EAPS shared port after an MSM failover.
PD4-2343129174, PD4-2038216594	If a port is included in an EAPS protected VLAN, it cannot be configured for redundancy.
Network Login	
PD4-2329221013, PD4-1324988340	The `configure netlogin dot1x timers supp-resp-timeout` command is incorrectly stored in the configuration file.
SNMP	
PD4-2345650880, PD4-2198529731	The snmpMaster process experiences memory depletion of approximately 4096 bytes per SNMP polling.

Table 45: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
Spanning Tree Protocol	
PD4-2383412020, PD4-2379771301	STP BPDU transmission can be delayed when a switch has a high CPU load.
PD4-2383412176, PD4-2336586249	Running STP timer `debug` commands on a large STP configuration may lead to system instability and failure with `signal 6`.

Resolved Issues in ExtremeXOS 12.6.2

The following issues were resolved in ExtremeXOS 12.6.2. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.6, ExtremeXOS 12.4.4, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 46: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-2260707781, PD4-2011056021	After a reboot, I/O slots do not go into an operational state with identity management enabled (when I/O ports are part of identity manager). **Workaround:** Using the ExtremeXOS CLI, run the `configure identity-management delete ports all` command before the switch reboots. Once the switch has rebooted, run the `configure identity-management add ports all` command.
PD4-2289644008, PD4-1933787334	The RtMgr process may encounter the assertion failure `ASSERTION FAILURE by rtmgr in rtMgrResolveEgressIf()@rtMgrTable.c:6892 REASON: IPGW_OUTIF_INDEX(tmpInfo) == ifIndex` when an IP address is configured on a VLAN.
PD4-1885958264	If the same two user names and domain names are detected via netlogin dot1x and kerberos, the identities are correlated and only one identity is created. If the same domain name supplied via netlogin and kerberos in different case, correlation does not occur because identity manager treats domain names as case-sensitive. In the MD5 or PEAP using MS-CHAPv2 method of dot1x, there is no domain name detected by netlogin. Therefore, only the user name without the domain is supplied to identity manager because identity manager treats “user1” and “user1@domain1” as different identities.
PD4-2260272816, PD4-2119506258	Loading a configuration from a script or pasting a configuration to a telnet session is not working for a specific set of PIM commands. **Workaround:** Change the order of the configuration so that the `configure vlan <vlan> tag <tag value>` command is placed between the `configure vlan <vlan> ipa <ip address>` and `configure pim add vlan < vlan > sparse` commands.
PD4-2177745625, PD4-2142352206	A switch reboots when auto-binding a management VLAN to STPD s0.
PD4-2191243961	Performing a hitless upgrade on a BlackDiamond 10800, 12800, or 20800 series switch to an ExtremeXOS 12.6 image is not successful because MSM-B fails to sync up with MSM-A.
PD4-2197499950, PD4-2037865872	sFlow throttling messages are logged even if the incoming packet rate is less than the sFlow sampling rate.

Table 46: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-2211004635, PD4-2204361206	An etmon process crash followed by an MSM failover occurs when receiving a corrupted packet from EPICenter.
PD4-2192405770, PD4-2052811367	A system experiences a crash when replacing option 82 parameters in a DHCP packet.
PD4-2191752617, PD4-2029508189	Unconfiguring port monitoring results in a VLAN process crash.
PD4-2240815039, PD4-2040737205	Redundant port configuration is blocked after unconfiguring a slot on a primary port.
PD4-2163527793	If a target Web server that is to receive XML notifications becomes non-responsive, unbounded buffering of pending notifications may occur in the switch and lead to an out of memory situation and a system reboot. If the target Web server is known to be out of service for an extended period of time, the applicable XML notification target should be disabled until the Web server is available for use.
PD4-2187239819, PD4-2101532349	The AAA process may crash with signal 6 when a user is connected to a switch using SSH and RADIUS is used for the user authentication.
PD4-2221727082, PD4-2221702811	A Summit series or BlackDiamond 8800 series switch reboots when receiving OAM packets larger than 60 bytes.
BlackDiamond 8800 Series Switches	
PD4-2260272645, PD4-2212482801	Ports on an 8500-G48T-e module should not be allowed to be part of a user created virtual router.
PD4-2155755740	Enabling load-sharing on 8900-40G6X-xm ports when in 4x10 partition mode fails when a combination of 40G capable and 10G ports are used in a group.
PD4-2249013181, PD4-1956113551	On a BlackDiamond 8800 series switch, CFM and STP packets generated by the switch are not sent out from the ports configured as PVLAN "translated" ports.
BlackDiamond 12800 Series Switch	
PD4-2244463201	Some BlackDiamond 12800 series MSM-6R modules cannot be upgraded to ExtremeXOS 12.4 or later.
BlackDiamond 20800 Series Switches	
PD4-2182155059, PD4-2181943197	An `eeprom local read` error message and an I/O module failure is displayed in the log of a BlackDiamond 20800 series switch.
Summit Family Switches	
PD4-2189098441, PD4-1920375601	Auto provisioning is not supported on Summit series switches with an L2 Edge license.
PD4-2198659042, PD4-2193875193	When connecting an AP4710 to a Summit X460-48p switch, the switch port does not come up to provide power.
PD4-2226859191, D4-1857577536	A switch shows the SSH status as "Module not loaded" when upgrading the switch from ExtremeXOS 12.1.5.1 to v1252b0-br-ssh-license-1 with Extreme Networks SSH software module (ssh.xmod) license file. **Workaround:** After upgrading to ExtremeXOS 12.5 software, uninstall and reinstall the SSH software module (ssh.xmod) and enable the SSH license
PD4-2192405831, PD4-2014131027	On a Summit X450a-24x series switch, an EAPS flush is not performed on a root blocker when a second link goes down.
PD4-2054838823	On a Summit X650 series switch with a VIM3-40G module, counters are not incremented when an ACL is applied to a VLAN and the ingress and egress ports are on a different ASIC.
PD4-1990330988	On a Summit X670 series stack, a stable stack is not formed when using 40-Gb stacking links.

Table 46: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
SummitStack	
PD4-2233266555, PD4-2057876228	UPM profile execution status remains in running state after a SummitStack failover.
PD4-2184877849	When using IdMgr, a switch is not syncing a dot1x identity domain and role information with a backup slot. The switch shows identity information without the role information, which is being left blank.
PD4-2209090695, PD4-1771248139	In some cases, an SSH key may not be check pointed to backup node on a SummitStack.
PD4-2211004528, PD4-2204361124	Cross ASIC multicast forwarding does not work using static FDB entries with learning, multicast flooding, and IGMP snooping disabled.
PD4-2221911417, PD4-2213319763	HAL stack utilization is approximately 98% and a stack overrun crash occurs when repeatedly configuring and unconfiguring an ACL with traffic.
PD4-2189094555, PD4-2112303228	An ELRP loop occurs after rebooting a Summit X450e-48p stack because of a delay in EAPS convergence.
PD4-1918982514	The motion sensor control for LED power savings is not working on Summit X670 switches.
PD4-1908119150	A SummitStack does not use the MAC address of the stack for ARP replies when communicating with other devices.
PD4-2133805181	Summit X450a-24t switches with IDM do not detect Kerberos user movement from one port to another.
ACL	
PD4-2253921953, PD4-2137222784	When a policy file is changed, the changes are not available after an MSM failover.
BGP	
PD4-2050362299	All BGP routes are denied when "match community" is used as part of a policy file.
OSPF	
PD4-2087108158, PD4-1196732534	Receiving an OSPF LSA ACK message with an invalid LSA type value causes an assertion failure in the OSPF process.

Resolved Issues in ExtremeXOS 12.6.1

The following issues were resolved in ExtremeXOS 12.6.1. ExtremeXOS 12.6 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, ExtremeXOS 12.0.5, ExtremeXOS 12.1.6, ExtremeXOS 12.2.2-patch1-12, ExtremeXOS 12.3.5, ExtremeXOS 12.4.4, and ExtremeXOS 12.5.4. For information on those fixes, see the release notes for the specific release.

Table 47: Resolved Issues, Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-1883558321	When using IdMgr, the `configure identity-management add port all` command is not enabling IdMgr on any ports. **Workaround:** Use the `configure identity-management add port <portlist>` command to enable IdMgr on ports.
PD4-2028980702, PD4-1900406099	In a private VLAN, broadcast packets are not forwarded after a network VLAN port is changed to a shared port.‘
PD4-2121248121, PD4-2012411531	BlackDiamond series and Summit family switches do not examine dot1p inner tags with a LAG.
PD4-1866206217, PD4-1299135401	Multicast traffic is dropped with an EAPS shared port configuration during an EAPS topology change.
PD4-2088325283, PD4-1679877595	UPM execution status is returned as Pass regardless of the status of other commands if the show command is in the UPM profile.
PD4-1990369532, PD4-1751958424	In CLI scripting, $READ inside a loop is not working and displays the following error: `Incorrect READ syntax Error: Read syntax`
PD4-1844559626	After configuring a banner, if a configuration with no banner is used, the banner configured earlier is displayed.
PD4-2033837907, PD4-2034092051	A system crash may be seen in switches using UPM to trigger a set of configurations whenever a user is successfully authenticated by way of a network login port.
PD4-2033837872, PD4-1441107715	The FDB process dies with signal 11 when creating a blackhole entry for a MAC address authenticated by network login.
PD4-2080394847, PD4-1961884891	A configuration created with UPM in non-persistent mode cannot be made persistent by issuing CLI configuration commands.
PD4-1624707485	In an IdMgr configuration, a DUT does not show unknown entries if a client or server port is configured with a static IP address and connected to an L2 network.
PD4-2036794041, PD4-1927210571	A supplicant attached to a netlogin port on an Extreme switch is not receiving EAPS FAIL messages if RADIUS is unavailable.
PD4-1863654217, PD4-1851065925	The `show fdb` command output does not show the pseudo-wire FDBs after a port is disabled and enabled.
PD4-1823016119, PD4-1090889907	High CPU utilization messages are not logged while SNMP traps are sent.
PD4-1887144161, PD4-1155806118	When an unknown vendor ID is sent in a RADIUS accept packet, the log message does not print the unknown vendor ID.
PD4-1920100060, PD4-1918575400	FDB process crashes with signal 6 when a superVLAN or Sub VLAN name contains 15 or more characters.
PD4-1956914232, PD4-1937052478	Telnet access profiles are blocking all IPv6 telnet connections.
PD4-1981933678, PD4-1374774241	The SNMP OID extremeCurrentTemperature does not return the current temperature of a switch. This is also seen when accessing the switch using ScreenPlay.

Table 47: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1891009467, PD4-1813024595	The `show configuration ip-fix` command does not return a configured flow-key if you only configure `src-ip/dest-ip`. It also removes the non-IP flow-key.
PD4-1981255927, PD4-1229634794	LACP packets are corrupted if the master port is mirrored on a SummitStack.
PD4-1986104397, PD4-1933787279	The Node Manager process consumes excessive CPU usage on a backup MSM when the system uptime reaches 994 days.
PD4-1963014380, PD4-1409846531	The icmp-type match condition for ICMPv6 is not supported on Summit family and BlackDiamond 8800 series switches.
PD4-1957143133, PD4-1034683284	You cannot load a script using a flow-redirect configuration when a VLAN is down. **Workaround:** Enable the VLAN and reconfigure the flow-redirect configuration.
PD4-1947222081, PD4-1937692011	Copying large configuration files through SCP fails.
PD4-1917632053, PD4-1857823251	A mismatch between a PIM multicast cache and a hardware binding results in traffic loss.
PD4-1983606435, PD4-1867264398	Running the save configuration command on an ExtremeXOS switch with a dual MSM, or a stack with a backup node, causes a memory leak in the CfgMgr process.
PD4-1884535497	An LX mini-GBIC is incorrectly detected as an FX/LX mini-GBIC. This applies only to Summit family switches and BlackDiamond 20800 series switches.
PD4-1701643346, PD4-1677893691	A telnet connection may be abruptly closed by a switch when multiple telnet connections are consecutively initiated in a short period of time.
PD4-1701643329, PD4-1555469451	DHCP Option 82 packets are dropped if VPLS is enabled on an egress interface.
PD4-1851793216, PD4-1323337297	A switch experiences memory depletion because of the HAL process when sending L2 traffic to a PVLAN with a continuous SA increment.
PD4-1846363979, PD4-1821932411	The following directories are viewable in a browser window when Web HTTP is enabled: • /scripts • /images • /assets • /com
PD4-1702117524, PD4-1417613295	The help text for the `configure fdb vpls agingtime` command displays the wrong possible values.
PD4-1701643466, PD4-1081411076	The CLI allows RIP configurations for L2 VLANs. After completing a RIP configuration, running the show rip interface command causes the RIP process to die with signal 11.
PD4-1701643416, PD4-1446804247	Multicast traffic is showing the incorrect dot1p replacement for CPU (slowpath) forwarded packets with TOS bits set at 7.
PD4-1701643401, PD4-1240910931	The cfgmgr crashes with signal 11 due to NULL pointer access.
PD4-1770347535, PD4-1738654681	ExtremeXOS software does not correctly recognize the following mini-GBIC modules: • 100FX/1000LX dual speed SFP, part number 4050-00020-02 • 100FX SFP, part number 4050-00030-03
PD4-1814536052, PD4-1741274969	A switch crashes with soc_dma_done_desc in the NVRAM dump.
PD4-1758919554, PD4-1517323275	The SSH process (exsshd) consumes 99% of CPU usage when running the `clear session` command after abruptly closing an SSH session (xterm client only).
PD4-1758727774, PD4-1695304439	After configuring an EMS xml-notification target, the name of the target is not included in the output of the `show configuration` command.

Table 47: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1859775721, PD4-1847511220	When running the SSH process (exsshd), CPU usage is excessive, and some SSH sessions are not cleared.
PD4-1741718248, PD4-1107340401	When TACACS is used for user authentication, the log message shows the wrong IP address of the user being authenticated.
PD4-1819371681, PD4-896535258	When a banner configuration file stored in a Windows environment is loaded, the banner configuration is not restored properly. Note: After unconfiguring a switch, the system banner message cannot be restored using a saved configuration. **Workaround:** Reconfigure the banner message.
PD4-1757733788, PD4-1453474837	IGMP membership query packets are seen on a port when IGMP is disabled but IGMP snooping is enabled. To resolve this issue, run the `disable igmp proxy-query vlan <vlan-name>` command.
PD4-1813267597, PD4-1239811496	Deleting a VLAN does not cleanup route entries learned by RIP through the VLAN.
PD4-1828332412, PD4-1809345751	The HAL process dies with signal 11 if the refresh policy fails and the following error is displayed: `Unable to find the flow redirect used with the redirect-name keyword, policy not installed`
PD4-1835754729, PD4-1177495965	XML API allows a user to create several VLANs using the same VLAN tag.
BlackDiamond 8800 Series Switches	
PD4-1878642172	Pseudo wire counters for Tx and Rx are not working on BlackDiamond 8900 series switches after a transport LSP path is changed.
PD4-1827550796, PD4-1147104931	A BlackDiamond 8800 series switch takes more than 30 minutes to boot up with VLAN aggregation configured.
PD4-1900222002, PD4-1873304831	ECMP related error messages are seen on BlackDiamond 8800 series switches when `enable iproute sharing` and LAG are configured on the switch.
PD4-1921505433, PD4-1548261276	On a BlackDiamond 8800 series switch, traffic is not being redirected by the primary LACP port when the secondary MSM with secondary ports is rebooted on LACP during a process kill.
PD4-1963014319, PD4-1688446379	FDB entries learned via LAG are not included in the output of the `show fdb stats ports all` command.
PD4-1983542737	VLAN switch fabric hardware programming fails to reprogram a trunk to the correct unit on an I/O module after an unexpected failover occurs.
PD4-1701643386, PD4-1655256488	BlackDiamond 8800 series switches report "conduit failures" during bootup if the switch is configured with diffserv replacement enabled for more ports, as well as diffserv replacement mapping.
PD4-1865375627, PD4-1854613879	On a BlackDiamond 8800 series switch, multicast packets are sent directly to the CPU instead of being forwarded in hardware.
BlackDiamond 12800 Series Switches	
PD4-2080718320	MSDP peers get struck in the listen state on core devices after upgrading from ExtremeXOS 12.5.3.9 to ExtremeXOS12.6.0.19 software.
PD4-2068851890, PD4-2065239242	A port is removed from a load sharing group after an MSM failover after increasing the number of multicast data packets hitting a CPU because of an invalid rendezvous point (RP) or other failure.
PD4-1820711622, PD4-1083288117	Disabling and re-enabling a port that is configured for 100 Mbps full duplex with an attached dual speed SFP (100FX/1000LX) results in connectivity issues. Note: Also see PD4-1736309253.

Table 47: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
BlackDiamond 20800 Series Switches	
PD4-1905529165, PD4-1536990491	When a BlackDiamond 20800 series switch is an EAPS master, port QP1 increments instead of port QP8.
Summit Family Switches	
PD4-1914383901	Traffic for a multiport FDB entry sent from one port is not received on the other port.
PD4-2001047151	On a Summit X670V-48x switch, the QSFP+ SR4 is not detected correctly.
PD4-1992976721	Remote mirroring functionality is not working on a Summit X670 series switch.
PD4-1951023951	Wide key ACLs cannot be installed on a Summit X670 series switch.
PD4-2113529603, PD4-2113075930	The `synchronize` command is not working properly when run on a Summit X460 stack.
PD4-2012749841, PD4-1437616911	When running the `configure ports medium <fiber/copper> auto <on/off> speed <speed> duplex <half/full>` command, the command is not retained when a switch reboots.
PD4-2068851986, PD4-1751144935	Changing the date and time on a switch is not persistent after running the `save` and `reboot` commands.
PD4-1591238321	VM tracking repository synchronization is not working properly when using a remote FTP server.
PD4-1895428088, PD4-1488841268	Traffic destined for a known MAC address in a member VLAN is being flooded on the ports of the network VLAN.
PD4-1943788355, PD4-1920719829	CLEAR-Flow rules are not getting hit when a match condition is configured for byte-count.
PD4-1955257867, PD4-1419136822	On a Summit X450a-24x switch, disabling two or more ports causes a port that is inserted as a 10/100/1000BASE-T SFP module to flap.
PD4-1971710450, PD4-1776441950	Software-controlled redundant ports may cause loops if a port is configured for redundancy after it is associated with an existing VLAN.
PD4-1969892806, PD4-1962933707	EMS takes approximately 1-minute to report power status on a Summit switch with a redundant PSU.
PD4-1926408407, PD4-1231665209	The output for the CLI command `show odometer` always shows values in the option card field even though there is no option card in the switch.
PD4-1926408254, PD4-1838754211	Power status is not displayed on a Summit X650 switch in ScreenPlay if both PSUs are present but only one is powered on.
PD4-1948432807, PD4-1661214241	A Summit family switch does not send a PSU related SNMP trap when a secondary PSU fails.
PD4-1864265861, PD4-1507160161	VPLS Tx and Rx counters are not incrementing on Summit X460 switches.
PD4-1819139162, PD4-1681984346	Traffic is not going over a tagged VPLS service VLAN if an untagged service VMAN is configured on the same port.
PD4-1863559586, PD4-1588054183	Summit X480 switches are not using EXP bits to map VLAN traffic to the correct QoS profile.
PD4-1844619105, PD4-1840662158	Clients are not able to reach each other through a tunnel after running the `clear fdb` command or a link flap occurs on an MPLS cloud (LSR).
PD4-1842342647, PD4-1254695518	When deleting a port from an ELRP configured VLAN, the switch displays errors after running the `save` and `reboot` commands.

Table 47: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description

PD4-1704766832, PD4-1687280681	IP multicast packets received on a service VMAN/VLAN may not be flooded through a VPLS tunnel.
	Workaround: Add the service VMAN/VLAN port to any IGMP snooping enabled VLAN and delete the port from that VLAN. For example:
	`configure vlan default add port 21 tagged`
	`configure vlan default del port 21`

SummitStack	
PD4-1867670001	VM-tracking synchronization status is complete before all policy files are downloaded to a switch.
PD4-1556789099	Memory depletion may occur when 100,000 routes flap among the 200,000 advertised routes.
PD4-1970091731	During testing, ELRP reports a loop and displays the following error message: `Duplicate packet forwarding encountered when VPLS service VLAN traffic traverses the MLAG Inter-Switch Connection on a SummitStack with X460.`
ACL	
PD4-2077107171, PD4-1856038101	A telnet access profile is not retained after running the `save` and `reboot` commands.
PD4-1899475193, PD4-1887057001	Running the `configure flow-redirect <redirectname> no-active/health-check` command resets a configured VR to a VR-Default.
PD4-1933226690, PD4-1933225935	The ACL action "copy-cpu-and-drop" is not copying EAPS control packets to the CPU.
PD4-1757734278, PD4-1274429658	Configuring a dynamic ACL with flow-redirect does not work after a switch reboot. **Workaround:** After rebooting the switch, delete and add the ACL.
BGP	
PD4-1726059489, PD4-1701554204	BGP and MSDP may not establish a secure TCP connection to their peers when an encrypted password contains a special character such as #.
DHCP	
PD4-2087108280, PD4-1394637671	A switch updates DHCP clients with `dhcp-lease-timer` instead of `netlogin-lease-timer` if the `dhcp-lease-timer` value is changed.
PD4-2027631804, PD4-1372389708	Running the `upload ip-security dhcp-bindings` command fails with the following error: `Object dhcpBindingsUpload does not support method set.`
PD4-1854155063, PD4-1578760166	Duplicate BOOTP OFFER and ACK packets are seen when ip-security dhcp-snooping is enabled on a port. **Workaround:** Disable `ip-security dhcp-snooping` to prevent duplication of DHCP OFFER and ACK packets.
PD4-1866206149, PD4-1813046514	DHCP snooping log messages display the incorrect port information when a LAG violation occurs.
EAPS	
PD4-1981687955, PD4-1870786111	Running the `disable netlogin port <slot:port>` command while the slot is down causes the switch to drop the packets received on that port in hardware if the ethernet-source-address is not learned. This affects EAPSv1 control packets because the ethernet-source-address in the EAPSv1 control packets is a special MAC and will never be learned.

Table 47: Resolved Issues, Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-1701643481, PD4-1676753651	EAPSv2 segment health-check packets received on a ring port may be dropped if the EAPS node on a Summit family or BlackDiamond 8800 series switch has a different EAPS shared port on any other ring ports.
ESRP	
PD4-2073557643, PD4-2053914004	Traffic on an ESRP master or member VLAN is forwarded in slowpath, which results in high CPU utilization when hardware ARP limits are exceeded.
IGMP	
PD4-2051283925, PD4-1374138231	The configured IGMP query interval timer does not take effect immediately. The timer takes effect only after the current interval expires.
OSPF	
PD4-2063215708	The following error message is seen in a switch when an OSPFv3 learned route is not installed in the routing table when disabling or enabling OSPFv3 in a designated router: `[OSPF-Default] Route 2a02:2028:ff00::1:0:6/128 via interface VL_CORE_BB_HH, neighbour 213.209.106.230 has an unspecified Nexthop. Not downloading Route.`
PD4-2087444772. PD4-2049272717	OSPFv3 crashes with signal 11 during an "inter area prefix lsa" refresh when the link connected to an OSPFv3 neighbor goes down and comes back up.
PD4-2068852026, PD4-2065239181	A CLI command to enable OSPF related SNMP traps is not available at this time.
PD4-2039218370, PD4-1997097831	OSPF process crashes with an assertion failure when using a virtual link configuration.
PD4-1835365017, PD4-1394061328	ABR stops translating AS external routes (type 7) to another area (type 5) after OSPF is configured with graceful restart.
PD4-1842213451, PD4-1524171924	Not all of the AS external routes in OSPF are getting installed in the route table.
ScreenPlay	
PD4-1910798581, PD4-913229871	API queries for RADIUS and TACACS do not return any values. Set is working properly, but a get returns empty.
SNMP	
PD4-1702117722, PD4-1598272292	The snmpMaster process crashes with signal 11 on NULL pointer access.
PD4-1702117707, PD4-1328651560	The CLI command `disable snmpv3 user default-user` does not disable default user access.
Spanning Tree Protocol	
PD4-2012749913, PD4-1780972901	Renaming a VLAN and deleting the STP domain to which it has an auto-bind relation, auto-binding it to a new STP domain displays the following error: `Error: Cannot enable auto-bind for vlan v2 to STP domain s2, it is the carrier vlan of STP domain s1`
VRRP	
PD4-1701643451, PD4-1664819101	VRRP gateways may get stuck in a dual master state when VRRP is run on a secondary IP falling under the same address class as the primary, but in a different subnet.